



# Fiscal Year 2008 Report



National  
Communications  
System





# National Communications System

Ensuring Essential Communications  
for the Homeland

Prepared by the Office of the Manager,  
National Communications System





As the National Communications System (NCS) marked its 45th year of service to the Nation, the organization continues its mission to protect and improve America's national security and emergency preparedness communications capabilities against a comprehensive array of emerging and persistent threats. In an era of terrorist threats and catastrophic hurricanes, floods, snowstorms, wildfires and earthquakes, the NCS remains ever-vigilant, collaborating daily with all levels of government and the communications sector to prepare for wide-ranging disaster scenarios and evaluate opportunities for response enhancement in real-time situations.

Impacting the NCS mission was the March 2008 release of the National Response Framework (NRF), which replaced the National Response Plan as the principal policy guiding government to prepare for and carry out a unified national response to disasters and emergencies. As one of the primary agencies responsible for the NRF's Emergency Support Function 2-Communications (ESF #2), the NCS worked in partnership with the Federal Emergency Management Agency (FEMA) to ensure the inclusion of key site access, security, and fuel support provisions for essential service providers within the framework.

The NCS successfully collaborated early this fiscal year with FEMA in mounting a swift and effective response to the California wildfires in October 2007. In addition, the NCS contributed its Communications Asset Database to track Government communications assets that emergency personnel can deploy in support of ESF #2, tested equipment functionality to provide backup communications capabilities to support ESF #2 events. NCS staff members participated in national level exercises to simulate emergency response procedures, and conducted targeted training during the year to prepare key staff members ultimately tasked to respond to incidents when FEMA activates ESF #2.


Readiness and planning was a major NCS concern in FY 2008. Addressing the current state of emergency preparedness communications capabilities, NCS leadership held a series of strategic planning sessions to prioritize work efforts. As a result, the NCS focused its efforts on access, security, and fuel; communications and electric power interdependencies; and next generation networks, advancing those priorities through the NCS' operational, policy, and technological mechanisms.

The 2008 hurricane season gave the NCS a chance to demonstrate real-life execution of its emergency response capabilities. The National Coordinating

Center for Communications (NCC), in conjunction with its government and communications industry partners, successfully performed its role as the NCS emergency response mechanism in tracking, analyzing, and assessing a series of storms—including Hurricanes Dolly, Gustav, and Ike. The NCC proactively communicated with ESF #2 team members, industry partners and other ESF elements to coordinate pre- and post-landfall staging of emergency communications equipment, obtain access and security support, and coordinate fuel delivery for numerous communications sites.

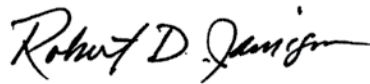
The NCS also placed significant emphasis on growing its longstanding intergovernmental and industry partnerships. In an on-going dialogue with the President's National Security Telecommunications Advisory Committee (NSTAC) and the NCS Committee of Principals (COP), the NCS developed a system for tracking and reporting government actions to implement the NSTAC's recommendations. As an example of one such action, the NCS COP hosted its Long Term Outage Workshop, April 8-9, 2008, in which participants from communications and electric power entities examined the dependencies between the two sectors and laid the groundwork to devise mitigation strategies. Additionally, the NCS spearheaded development of the Communications National Sector Risk Assessment between the Government Coordinating Council and the Sector Coordinating Council, building upon the Communications Sector Specific Plan.

Furthermore, members of the government and industry Network Security Information Exchanges represented the U.S. communications sector at the annual trilateral meetings with the United Kingdom and Canada. Finally, the NCC physically co-located its facilities with those of the National Cyber Security Division's U.S. Computer Emergency Readiness Team



to better facilitate information sharing on converging security concerns of the communications and information technology sectors.

Over this past fiscal year, the NCS continued to strategically blend action across national security and emergency preparedness priorities to challenge the ever-evolving threats to the Nation's security posture. With the growing demand for communications services within the Nation, the NCS will continue to lead Federal efforts to ensure that emergency communications remain readily available—not only during emergencies, but on a day-to-day basis. I trust that through the robust collaborative relationships with member agencies and industry partners, the NCS will continue to strengthen the resiliency of the Nation's communications infrastructure through innovative and effective solutions as it has for over 45 years.



Robert D. Jamison  
Manager  
National Communications System





Mr. Gregory T. Garcia  
**Deputy Manager**



Mr. James J. Madon  
**Deputy Manager  
and Director**



Mr. Allen F. Woodhouse  
**Chief of Staff and  
Acting Chief, Customer  
Service Branch**



Mr. Robert D. Jamison  
**Manager**



Mr. Nicholas Andre  
**Acting Chief, Technology  
and Programs Branch**



Mr. Jeffrey A. Glick  
**Chief, Critical Infrastructure  
Protection Branch**



Mr. James G. Bittner  
**Chief, Plans and  
Resources Branch**



## NCS Leadership

# NCS Committee of Principals



**Department of State (DOS)**  
Ms. Kimberly A. Godwin



**Department of the Treasury (TREAS)**  
Ms. Vicki Waizenegger



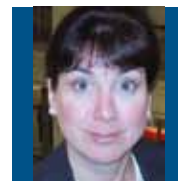
**Department of Defense (DOD)**  
Dr. John G. Grimes



**Department of Justice (DOJ)**  
Mr. Eric Olson



**Department of the Interior (DOI)**  
Mr. Timothy Quinn



**Department of Agriculture (USDA)**  
Ms. Susan A. Moore



**Department of Commerce (DOC)**  
Ms. Suzanne Hilding



**Department of Health and Human Services (HHS)**  
Mr. Gary Wall



**Department of Transportation (DOT)**  
Mr. Daniel G. Mintz



**Department of Energy (DOE)**  
Mr. Carl S. Pavetto



**Department of Veterans Affairs (VA)**  
Mr. Andres A. Lopez



**Department of Homeland Security (DHS)**  
Mr. Michael Brown



**Office of the Director of National Intelligence (ODNI)**  
Mr. Dale W. Meyerrose



**Federal Emergency Management Agency (FEMA)**  
Ms. Martha Rainville



**The Joint Staff (JS)**  
VADM Nancy Brown, USN



**General Services Administration (GSA)**  
Mr. James Williams



**National Aeronautics and Space Administration (NASA)**  
Ms. Betsy Edwards



**Nuclear Regulatory Commission (NRC)**  
Mr. Roy Zimmerman



**National Telecommunications and Information Administration (NTIA)**  
Ms. Meredith Baker



**National Security Agency (NSA)**  
Mr. Anthony Cornish



**Federal Reserve Board (FRB)**  
Mr. Kenneth D. Buckley



**Federal Communications Commission (FCC)**  
Mr. Kenneth P. Moran



**United States Postal Service (USPS)**  
Mr. Harold A. Stark





**Department of State (DOS)**  
Ms. Kimberly A. Godwin



**Department of the Treasury (TREAS)**  
Ms. Vicki Waizenegger



**Department of Defense (DOD)**  
Mr. Bill Gunnels



**Department of Justice (DOJ)**  
Mr. Gary Laws



**Department of the Interior (DOI)**  
Mr. Stuart A. Ott



**Department of Agriculture (USDA)**  
Mr. Roy Allums



**Department of Commerce (DOC)**  
Mr. Earl Neal



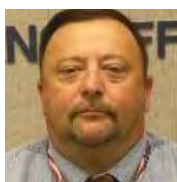
**Department of Health and Human Services (HHS)**  
Mr. Gary Wall



**Department of Transportation (DOT)**  
Mr. Michael Dammeyer



**Department of Energy (DOE)**  
Mr. Al Cerrone



**Department of Veterans Affairs (VA)**  
Mr. James Lacey



**Department of Homeland Security (DHS)**  
Mr. Keith Jones



**Office of the Director of National Intelligence (ODNI)**  
Ms. Sherrill L. Nicely



**Federal Emergency Management Agency (FEMA)**  
Mr. Rex Whitacre



**The Joint Staff (JS)**  
LTC Susan Camoroda, USA



**General Services Administration (GSA)**  
Mr. David Jarrell



**National Aeronautics and Space Administration (NASA)**  
Ms. Betsy Edwards



**Nuclear Regulatory Commission (NRC)**  
Mr. Stanley Wood



**National Telecommunications and Information Administration (NTIA)**  
Mr. Stephen Veader



**National Security Agency (NSA)**  
Mr. Anthony Cornish



**Federal Reserve Board (FRB)**  
Mr. Sheree D. Jones



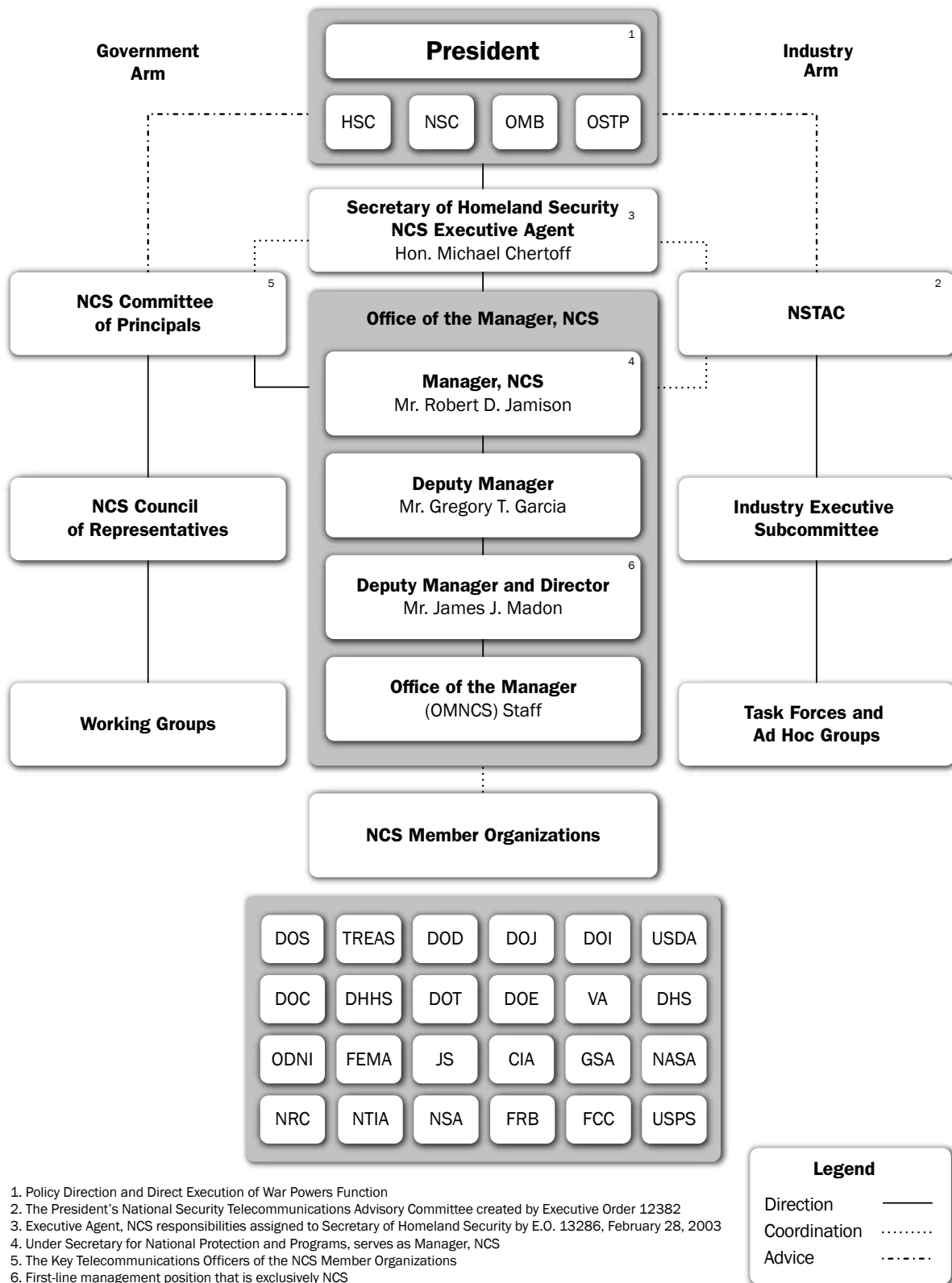
**Federal Communications Commission (FCC)**  
Mr. Allan Manuel



**United States Postal Service (USPS)**  
Mr. Warren Schwartz



# NCS Council of Representatives





# Table of Contents

<b>I</b>	<b>Introduction: The History of the National Communications System</b>	
	Background .....	2
	NCS Environment .....	3
	National Security Agency (NSA) .....	88
	Federal Reserve Board (FRB) .....	92
	Federal Communications Commission (FCC) .....	94
	United States Postal Service (USPS) .....	96
<b>II</b>	<b>Emergency Response Activities</b>	
	Hurricane Season 2008 .....	8
	Other Events .....	10
<b>III</b>	<b>NS/EP Telecommunications Support, Activities, and Programs</b>	
	Technology and Programs Branch .....	12
	Critical Infrastructure Protection Branch .....	27
	Plans and Resources Branch .....	37
	Customer Service Branch .....	37
<b>IV</b>	<b>NS/EP Telecommunications Support And Activities of Member Organizations</b>	
	Department of State (DOS) .....	50
	Department of the Treasury (TREAS) .....	54
	Department of Defense (DOD) and Joint Staff (JS) .....	59
	Department of Justice (DOJ) .....	65
	Department of the Interior (DOI) .....	66
	United States Department of Agriculture (USDA) .....	68
	Department of Commerce (DOC) .....	69
	Department of Health and Human Services (HHS) .....	71
	Department of Transportation (DOT) .....	72
	Department of Energy (DOE) .....	73
	Department of Veterans Affairs (VA) .....	74
	Department of Homeland Security (DHS) .....	75
	Office of the Director of National Intelligence .....	78
	Federal Emergency Management Agency (FEMA) .....	79
	Central Intelligence Agency (CIA) .....	81
	General Services Administration (GSA) .....	82
	National Aeronautics and Space Administration (NASA) .....	84
	Nuclear Regulatory Commission (NRC) .....	85
	National Telecommunications and Information Administration (NTIA) .....	86
<b>A</b>	<b>NCS-Related Acronyms</b> .....	<b>99</b>
<b>B</b>	<b>Photo Credits</b> .....	<b>105</b>





## Introduction: The History of the National Communications System





# Introduction: The History of the National Communications System

## Background

The Office of the Manager, National Communications System (OMNCS), prepared this report to describe the agency's national security and emergency preparedness (NS/EP) activities and telecommunications events, including highlights of the agency's innovations, programs, and achievements during fiscal year (FY) 2008.



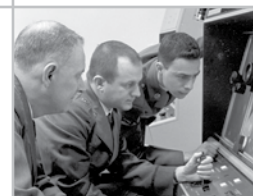
Meeting of the Executive Committee of the National Security Council—Cuban Missile Crisis. President Kennedy, Secretary of State Dean Rusk, Secretary of Defense Robert S. McNamara. White House, Cabinet Room. (Kennedy Library)

During the 1962 Cuban Missile Crisis, the United States, the Union of Soviet Socialist Republics, the North Atlantic Treaty Organization, and foreign heads of state experienced difficulties establishing and maintaining vital communications. To remedy these communications challenges after the crisis, President John F. Kennedy ordered the National Security Council (NSC) to conduct an investigation of the critical national security communications. As a result of its study, the NSC recommended the creation of a consolidated system to support Government communications functions. President Kennedy supported this recommendation by signing National Security Action Memorandum 252, establishing the National Communications System (NCS) on August 21, 1963. Further, the memorandum directed the NCS mission to be to “provide the necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies, and international crises, including nuclear attack.”

For over 45 years, the NCS mission has evolved steadily with telecommunications' expanding role in supporting national NS/EP functions, reinforcing that the Nation's telecommunications infrastructure is an essential component of deterrence and recovery in the event of an attack. The divestiture of AT&T and the emergence of network technology capabilities in the early 1980s greatly changed the Nation's security communications landscape by expanding the domestic telecommunications market. Consequently, this expansion further complicated the means for satisfying the Federal Government's NS/EP requirements.

To address those changes in the telecommunications environment, President Ronald Reagan signed Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, on April 3, 1984. The executive order modified the NCS structure to include the Secretary of Defense as the Executive Agent; the designation of an NCS Manager and staff; and a Committee of Principals (COP) to represent the Federal member organizations with NS/EP responsibilities. E.O. 12472 revised the mission of the NCS, requiring it to assist the Executive Office of the President, including the NSC; the Office of Science and Technology Policy; and the Office of Management and Budget in the exercise of all-hazards emergency telecommunications responsibilities. Additionally, the executive order tasked the NCS to coordinate the planning and provisioning of NS/EP communications for the Federal Government under all circumstances.

The terrorist attacks on September 11, 2001, forever altered the national threat landscape and demonstrated an immediate need for increased awareness and decisive action. On October 8, 2001, President George W. Bush issued E.O. 13228, *Establishing the Office of Homeland Security (OHS) and the Homeland Security Council*. The E.O. tasked the OHS with coordinating protection efforts for critical public and privately owned information systems within the United States. E.O. 13228 also gave the OHS authorization to coordinate efforts to provide the rapid restoration of telecommunications and critical information systems after disruption by a terrorist threat or attack.



Two beams of light represent the former Twin Towers of the World Trade Center during the 2004 memorial of the September 11, 2001 attacks. (Photo by Derek Jensen/Tysto)

Eight days after issuing E.O. 13228, President Bush issued E.O. 13231, *Critical Infrastructure Protection*, establishing the President's Critical Infrastructure Protection (CIP) Board. E.O. 13231 re-established the NCS COP as a permanent standing committee with additional reporting requirements to the new CIP Board. Furthering the Government's focus on homeland security, on November 25, 2002, President Bush signed into law the *Homeland Security Act of 2002*. Signaling the largest Government reorganization in 50 years, the act established the Department of Homeland Security (DHS) and restructured all Government departments and agencies with homeland security missions.

On February 28, 2003, the President signed omnibus E.O. 13286, *Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*, which transferred certain agencies and agency components to fall under the Department of Homeland Security. E.O. 13286 transferred the NCS Executive Agent responsibilities from the Department of Defense to DHS, and the NCS officially became a part of DHS on March 1, 2003. In its early years, DHS aligned the NCS under the Information Analysis and Infrastructure Protection Directorate. Later, the department moved the NCS under the Office of Cyber Security and Telecommunications within the Department's Preparedness Directorate in 2005.

Subsequently, the *Department of Homeland Security Appropriations Act of 2007* included several provisions requiring DHS organizational change. One provision included the establishment of the National Protection and Programs Directorate (NPPD) and the renaming of the Office of Cyber Security and Telecommunications as the Office of Cybersecurity and Communications (CS&C). As a result, DHS aligned the NCS under CS&C within NPPD.

## NCS Environment

The NCS engaged in a number of activities in FY 2008. In some cases, these activities were continuations and enhancements of ongoing efforts. In other cases, the NCS responded to the continually evolving environment by pursuing new initiatives. In combination, the activities struck a balance between the NS/EP dimensions of the NCS mission.

During FY 2008, the NCS completed a range of technological, operational, and policy activities related to these areas that focused on improving the Nation's NS/EP posture. The NCS agenda focused on incorporating Next Generation Networks (NGN) and evolving technologies into the NS/EP framework. The NCS examined telecommunications and electric power interdependencies, continued its longstanding support of intergovernmental and industry partnerships, and



coordinated access, security, and fuel for essential service providers—especially critical during Hurricanes Gustav and Ike.

### Access, Security, and Fuel

The National Response Framework (NRF) encourages the ongoing development and refinement of all-hazards emergency operations plans, with a focus on measures to ensure that emergency responders have the access, security, and fuel responders need to fulfill their missions. The NRF provides guidance for implementing national-level policy and coordination during incident response and defines the corresponding roles, responsibilities, and relationships. As part of that effort, the NCS, through its National Coordinating Center for Communications, plays a large part in expanding the capabilities needed to fulfill the emergency communications responsibilities set forth in the NRF's Emergency Support Function 2-Communications (ESF #2) Annex. As specified in the NRF, the ESF #2 responsibilities include coordinating with industry to provide communications support to Federal, State, local, and tribal governments and first responders during incidents that require a national-level response.



Dave Garrett, (left) FEMA Deputy Administrator and Ruben Almaguer, Deputy Director, Florida Division Emergency Management receive a briefing on the FEMA Mobile Disaster Recovery (MDRC) capabilities from Chris Christiansen, (right) MDRC Program Liaison. The vehicle and its communication tools are on display at FEMA's Emergency Support Function (ESF) Conference in Tampa, Florida, June 4, 2008. (Photo by Barry Bahler/FEMA)

NCS staff members received valuable ESF #2 training during the Federal Emergency Management Agency (FEMA) National Exercise Program's National Level Exercise 2-08 in May 2008. The exercise included injects requiring exercise participants to coordinate access, security, and fuel for industry essential service

providers, allowing NCS staff to simulate emergency response procedures. This event also staged several scenarios that exercised national capabilities to prepare for and respond to various natural disasters and terrorist incidents.

All training scenarios explore incidents that could disrupt communications infrastructure supporting critical Government facilities and demonstrate the importance of strengthening critical NS/EP communications technology resiliency.

### Next Generation Networks (NGN) and Evolving Technologies

The NCS aimed to enhance its technology-based programs in FY 2008, particularly emphasizing the transition to the NGN environment. The NCS is focusing on enhancing the effectiveness and capabilities of the Wireless Priority Service (WPS), the Government Emergency Telecommunications Service (GETS), and the Telecommunications Service Priority programs. The NCS continues to ensure continuity of WPS and GETS as the telecommunications infrastructure transitions to a packet-switched NGN. To continue to shape the future of these priority program service offerings, the NCS engages in a number of activities in the areas of NGN architecture development, modeling and analysis, prototyping, and industry requirements. Specifically, NCS engineers are investigating the use of wireless access technologies and the Internet Protocol Multimedia Subsystem (IMS) framework to evaluate possible NS/EP communications modeling scenarios. In addition, they are developing models and simulations of IMS core, carrier backbone, and various access networks to evaluate NS/EP enhancements for the NGN GETS industry requirements. The NCS also continues to use the Next Generation Priority Service Experimental Test Bed Environment to test end-to-end operation of next generation services.

### Telecommunications and Electric Power Interdependencies

The NCS addressed telecommunications and electric power interdependencies in long-term outage situations for both the current and future NGN environment when its COP hosted a Long Term Outage Workshop in April 2008. The workshop followed the 2006 President's National Security Telecommunications Advisory Committee Report to the President on Telecommunications and Electric Power Interdependencies, which provided an evaluation of technological interdependencies that will affect the

telecommunications infrastructure in the future. Coordination among workshop participants reinforced relationships among government and industry entities. Participants from communications and electric power entities examined the dependencies between the two sectors and laid the groundwork to devise mitigation strategies.

## NCS Partnerships

The NCS recognizes the value of collaboration with government and industry partners to ensure effective telecommunications response, recovery, and coordination. The Communications Sector-Specific Plan called for developing a risk assessment methodology to assess physical and cyber threats, in accordance with the 2003 Homeland Security Presidential Directive-7 and the 2006 National Infrastructure Protection Plan. To achieve this objective, the NCS worked with the Communications Sector Coordinating Council and Communications Government Coordinating Council to develop the *National Sector Risk Assessment* for the communications infrastructure. The risk assessment is a component of the sector's overall infrastructure protection plan that will drive more risk assessments, new programs, and research and development. It is the first sector-wide qualitative risk assessment examining physical and cyber threats to the communications infrastructure.

The NCS continues its involvement in the Network Security Information Exchanges (NSIE), where industry and Government voluntarily share sensitive information on threats to operations, administration, maintenance, and provisioning systems supporting the telecommunications infrastructure. In the past, NSIE members attended annual trilateral meetings with similar information-sharing entities representing the United Kingdom and Canada. In June 2008, the NSIEs invited Australia and New Zealand to attend the 2008 trilateral meeting as guests, laying the groundwork to expand multilateral collaboration in the future.

The NCS continues to ensure the availability and resilience of NS/EP communications services by developing strategies to respond to emerging policies, technologies, and threats that influence the Nation's telecommunications infrastructure. As it has for decades, the NCS also fosters productive industry-Government partnerships to address national security risks. As the evolving communications environment continues to introduce new challenges, the NCS remains poised to lead the collaborative effort to strengthen the national communications posture.









## Emergency Response Activities

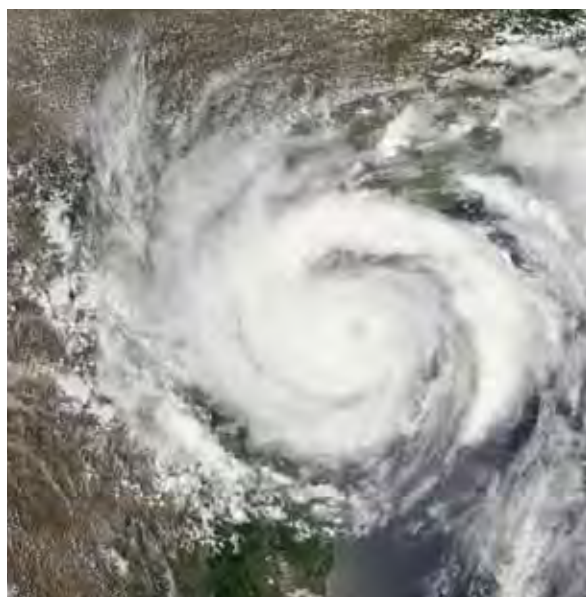


# Emergency Response Activities

## Hurricane Season 2008

During the 2008 hurricane season, 16 storms formed in the Pacific Ocean, and 17 formed in the Atlantic. Of the 17 storms in the Atlantic, four hurricanes and three tropical storms threatened and/or made landfall in the United States. The National Communications System (NCS) monitored all storms and three of these, Tropical Storm Cristobal, Tropical Storm Edouard, and Hurricane Hanna, had very little impact to the infrastructure.

The Federal Emergency Management Agency (FEMA) activated the National Response Framework's Emergency Support Function 2-Communications (ESF #2) six times during the hurricane season. The Gulf Coast Region was hit especially hard by Hurricanes Dolly, Gustav and Ike, all which made landfall as Category 2 hurricanes on the Saffir-Simpson Scale. There were significant impacts on communications assets due to these hurricanes. The National Coordinating Center (NCC) maintained a high alert posture throughout the hurricane season and monitored, analyzed, and assessed all approaching storms. Through the efforts of the NCC, the NCS was able to assist in the timely restoration of communications in the impacted areas.



Hurricane Dolly intensified to a Category 2 storm in the Gulf of Mexico, just before it bore down on South Padre Island off the South Texas coast. (Moderate Resolution Imaging Spectroradiometer [MODIS] on NASA's Terra satellite, Jesse Allen and Rebecca Lindsey)

## Hurricane Dolly

Dolly became a tropical storm in the Caribbean Sea off the coast of Mexico on July 20, 2008. The storm made landfall in Mexico on July 21 and then moved into the Gulf of Mexico. Dolly strengthened to a hurricane on July 22 and made landfall on South Padre Island in Texas on July 23 as a Category 2 hurricane with 100 mile-per-hour (mph) winds. FEMA activated ESF #2 to Level 1 with 24x7 operations at the FEMA National Response Coordinating Center (NRCC) and the Region IV Regional Response Coordinating Center (RRCC). Throughout Dolly's path, the NCC participated in daily FEMA leadership conference calls as a means of maintaining situational awareness, and held daily conference calls with industry and Government representatives to facilitate information sharing and coordinate pre-landfall and post-landfall activities. Multiple power and communications impacts were sustained but mitigated due to preparedness level of both the State of Texas and the resilience of the communications infrastructure.



FEMA's Ron Thomas, Denton, Texas, sets up the Incident Response Vehicle (IRV) for communications in Weslaco, Texas, on July 24, 2008 following Hurricane Dolly. (Photo by Barry Bahler/FEMA)



## Tropical Storm Fay

Fay became a tropical storm on August 15, 2008, and made its first landfall in Florida on August 18. Fay eventually made landfall in Florida four times as the storm moved back and forth across Florida and finally into Alabama. The Federal Communications Commission (FCC) initiated the Disaster Information Reporting System (DIRS) for the first time to report communications outages. The NCC participated in daily FEMA leadership conference calls as a means of maintaining situational awareness, and held daily conference calls with industry and Government representatives to facilitate information sharing and coordinate pre-landfall and post-landfall activities.



Crews collect debris piled at the side of the road by residents of Galveston, Texas, as they toss away drywall, insulation and personal possessions damaged by Hurricane Ike on September 29, 2008. (Photo by Robert Kaufmann/FEMA)

## Hurricane Gustav

Gustav became a tropical storm on August 25, 2008, in the Caribbean Sea and quickly strengthened to a hurricane on August 26. Gustav peaked as it made landfall in Cuba as a Category 4 hurricane with maximum wind speeds of 150 mph. After crossing Cuba, Gustav moved across the Gulf of Mexico and made landfall on the southern Louisiana coast near Cocodrie on September 1 as a Category 2 hurricane. This was the first major hurricane to hit Louisiana since Hurricane Katrina in 2005. Gustav tested the response efforts of the state and Federal governments. The FCC initiated DIRS for reporting communications outages. Additionally, ESF #2 was activated to Level 1 with 24x7 operations at the NRCC and the Region IV and Region VI RRCC. The NCC took part in daily

FEMA leadership conference calls as a means of maintaining situational awareness. The NCC also held daily conference calls with industry and Government representatives to facilitate information sharing and coordinate pre-landfall and post-landfall activities. Additionally, prior to landfall, a cadre of ESF #2 personnel were deployed to the NRCC, and RRCCs in both Denton, Texas and Baton Rouge, Louisiana.

## Hurricane Ike

On September 1, 2008, Ike became a tropical storm as it moved west across the Atlantic Ocean. By September 4, it had strengthened to a Category 4 hurricane with peak winds of 145 mph. Ike weakened



A power crew replaces a pole broken by Hurricane Ike in Houston, Texas, on October 11, 2008. (Photo by Greg Henshall/FEMA)

to a Category 1 hurricane as it moved across Cuba and into the Gulf of Mexico. Once in the gulf, Ike regained strength and made landfall in Galveston, Texas, on September 13 as a Category 2 hurricane. The FCC initiated DIRS for reporting communications outages. Additionally, FEMA activated ESF #2 to Level 1 with 24x7 operations at the NRCC and Region VI RRCC. Throughout Ike's track, the NCC participated in daily FEMA leadership conference calls as a means of maintaining situational awareness, and held daily conference calls with industry and Government representatives to facilitate information sharing and coordinate pre-landfall and post-landfall activities. NCS personnel were deployed to the NRCC, the RRCC and the Joint Field Office in Austin, Texas, to assist in recovery efforts. The NCS coordinated with local government and industry to quickly respond to major damages to the communications infrastructure, particularly on Galveston Island.





Northern California fire crews in San Diego set fire back burn to stop the Poomacha fire from advancing westward. By October 26, 2007, the fires in Southern California had burned more than 355,000 acres. (Photo by Andrea Booher/FEMA)

## Other Events

Notwithstanding a relatively active hurricane season, the NCS also supported response efforts for a number of other events. Specifically, the NCC Watch performed infrastructure analyses to determine the impact to telecommunications assets for the following events:

- ▶ California Wildfires, June 2008 to present;
- ▶ State of the Union Address, January 28;
- ▶ Super Bowl XLII, February 3;
- ▶ Middle East Cable Cuts, January-February;
- ▶ New York City GPS Interferences, April;
- ▶ Iowa Floods, June;
- ▶ Democratic National Convention, August 25-28; and
- ▶ Republican National Convention, September 1-4.

The NCC Watch notified and distributed relevant situation reports to the appropriate Communications Information Sharing and Analysis Center (ISAC) members during these events. In addition to these minor emergency response events, the NCC Watch participated in a number of cyber events during Fiscal Year 2008. The role of the NCC Watch in these cyber events was to distribute information advisories to Communications ISAC members and provide coordination and situational awareness to appropriate organizations, such as the Department of Defense's Joint Task Force for Global Network Operations and the United States Computer Emergency Readiness Team.



## NS/EP Telecommunications Support, Activities, and Programs



# NS/EP Telecommunications Support, Activities, and Programs

This section highlights the activities and accomplishments of the Office of the Manager, National Communications System (OMNCS) and the national security and emergency preparedness (NS/EP) community during fiscal year (FY) 2008.

## Technology and Programs Branch

The Technology and Programs Branch develops programs, technical studies, modeling capabilities/analyses, and standards that promote the reliability, security, interoperability, and priority treatment of NS/EP telecommunications. Branch objectives stress incorporating advanced, cost-effective technology into NS/EP communications programs and evaluating emerging technologies to alleviate impediments to interoperability. The NCS brings this information to industry and international standards organization meetings to ensure that recommendations incorporate NS/EP requirements.

The following sections highlight the major projects undertaken by the Technology and Programs Branch during FY 2008.

## Government Emergency Telecommunications Service

### Background

The NCS established the Government Emergency Telecommunications Service (GETS) to meet White House requirements for a survivable, interoperable, nationwide voice band service for authorized users engaged in NS/EP missions. GETS satisfies these requirements by providing specialized processing in local and long distance public telephone networks. Reaching full operational capability on September 30, 2001, the GETS program continues to ensure that NS/EP users receive a high rate of successful call completion during network congestion or outages arising from natural or manmade disasters. The GETS design focuses on the public switched telephone network (PSTN) as the most



efficient, reliable, and robust technology infrastructures for supporting a service that would meet NS/EP mission requirements.

In addition to implementing priority treatment and enhanced routing features in the interexchange carriers (IXCs) AT&T, Verizon Business, and Sprint Nextel and local exchange carriers (LECs) networks, the NCS worked with the American National Standards Institute (ANSI) to ensure NS/EP calls receive priority in the Signaling System 7 (SS7) networks. ANSI approved the High Probability of Completion (HPC) Standard ANSI T1.631-1993, which provided a classmark for NS/EP-related signaling messages. At least 90 percent of the access lines in the Nation now have the capability to process GETS calls.

### Functional Description

GETS users access the program by way of a priority calling card. When a user dials the GETS universal access number, a tone prompts for a GETS personal identification number (PIN). Next, a voice recording asks for a destination telephone number. In the event the access control system is inoperative, a fail-open feature will allow users to complete their GETS PSTN calls.

### GETS Benefits to the NS/EP Community

Within the last three years, the largest disasters occurred due to the devastating hurricanes of 2005, Katrina, Rita, and Wilma. Over 40,000 GETS calls originated or terminated in the affected areas, and the NCS issued over 2,000 new GETS cards to support related NS/EP activities, and achieved over a 95-percent completion rate.

During the various FY 2008 disasters, such as the floods in the mid-west, wildfires in the west and numerous hurricanes, and also during events such as the Democratic and Republican political conventions, the average GETS call completion rate was 97.4 percent.

### FY 2008 Accomplishments and Improvements

In the past year, the GETS program continued to make significant progress in its outreach efforts to all levels of government (Federal, State, local, and tribal) and other qualified NS/EP industry and non-profit

organizations. As of September 15, 2008, there were 206,841 active GETS cards—an increase of 38,917 cards since September 17, 2007. The NCS Service Center personnel processed and expedited 851 emergency activations after normal duty hours during critical FY 2008 events.

GETS NS/EP Category	GETS NS/EP Users
Federal	98,992
State/Tribal	23,650
U.S. House & Senate	822
Local	41,017
Industry	41,185
Other NS/EP organizations	1,175
Total	206,841

Table 1. GETS User Breakdown

## Highlights and Status of Ongoing Activities

The NCS continues to expand GETS capabilities in the PSTN and participates in activities that facilitate these efforts:

- ▶ The GETS Integration Contractor (IC) is working with additional service providers to provide GETS capabilities in their networks (such as CenturyTel, TDS Telecom, Time Warner Telecom, and Alaska telephone companies) and is in discussions with several additional carriers to obtain agreements to deploy GETS capabilities.
- ▶ To ensure the NCS is meeting NS/EP needs as the PSTN evolves to the next generation networks (NGN), the GETS IC continues to work with Sonus Networks to enhance NS/EP features in its NGN products.
- ▶ The NCS hosted a GETS/Wireless Priority Service (WPS) Team Forum in May 2008 for service providers, vendors, and other industry participants to inform them of NCS activities, especially related to the NCS industry requirements effort on NS/EP NGN priority capabilities. NGN issues are discussed in detail later in this document in the section titled “NS/EP Priority Services in Next Generation Networks (NGN).”
- ▶ The NCS continues to participate in the Alliance for Telecommunications Industry Solutions (ATIS)

Network Interconnection Interoperability Forum (NIIF) to promote NS/EP needs. The NCS works with the ATIS NIIF on inter-carrier network signaling and management procedures used during times of network traffic congestion.

## Partnership Activities

**Federal Departments and Agencies**—The NCS coordinates with sections of the Executive Office of the President (EOP)—including the Homeland Security Council (HSC), National Security Council (NSC), Office of Management and Budget, and Office of Science and Technology Policy (OSTP)—to provide NS/EP priority telecommunications to the Federal Government. In operating GETS, the NCS coordinates with the 24 Federal departments and agencies that comprise the NCS membership (see [http://www.ncs.gov/mem\\_orgs.html](http://www.ncs.gov/mem_orgs.html) for details) as well as other departments and agencies as appropriate.

**State and Local Agencies and Organizations**—GETS users include State and local government organizations and officials supporting emergency preparedness and response.

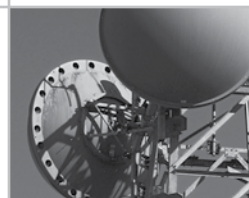
**Private Sector**—The NS/EP community supporting NS/EP mission requirements includes industry and non-government emergency response organizations plus industry owners and operators of critical infrastructures, such as nuclear facilities, regional and national airports, ports, railroad communications, and information technology.

**International**—GETS serves components of the Department of Defense and Department of State, to include U.S. embassies worldwide, and supports the financial services sector by providing GETS to international central banking entities. GETS also serves strategic international allies of the United States, including Canada and the United Kingdom.

## Wireless Priority Service

### Background

WPS is a nationwide wireless telephone service that interoperates with GETS and provides priority NS/EP telecommunications via selected commercial mobile radio service (CMRS) providers. Like GETS, WPS supports NS/EP emergency response and recovery operations.





WPS provides end-to-end nationwide wireless priority communication capabilities to key NS/EP personnel during natural or man-made disasters or emergencies that cause congestion or network outages in the commercial cellular network. WPS is complementary to, and most effective when used in conjunction with, GETS to ensure a high probability of call completion in both the wireless and wireline portions of the public networks.

In response to an October 1995 petition from the NCS, the Federal Communications Commission (FCC) released a Second Report and Order (R&O) [FCC-00-242, July 13, 2000] on wireless Priority Access Service (PAS), enabling WPS to be developed.

During the days following the terrorist attacks of September 11, 2001, the NCS issued guidance to the NCS regarding the development and implementation of WPS.<sup>1</sup> Responding to this guidance, the NCS provided an off-the-shelf, immediate WPS (I-WPS) solution, with limited capabilities in place for the February 2002 Winter Olympics in Salt Lake City, Utah. By December of that year, the NCS achieved nationwide WPS capabilities within the first carrier network, T-Mobile.

NS/EP users are currently able to subscribe to WPS in nearly all the major wireless markets in the continental United States and in U.S. territories served by the major nationwide carriers (AT&T Mobility, Sprint Nextel, T-Mobile, and Verizon Wireless).



## Functional Description

WPS is a subscription-based service that enables properly authorized and enrolled NS/EP users to invoke WPS on a per-call basis. Unlike GETS (which uses a personal identification number-based authentication), WPS uses a \*272 feature code prefix plus the destination number to originate and authenticate a WPS call.

WPS provides queuing to congested PSTN interfaces for calls originated at a mobile switching center (MSC) and traversing another carrier's network. Regardless of whether a WPS call traverses the PSTN or simply connects within the same MSC, queuing is also applied when terminating a WPS call into a cell where all radio channels are busy. WPS and GETS integration provides an end-to-end priority treatment for NS/EP calls, including calls that originate, transit, and/or terminate in wireless and/or landline networks.

WPS priority functionality in the commercial cellular networks includes priority-based radio access queuing, trunk queuing, priority-based radio egress queuing, and enhanced routing schemes, while preserving the capability for public access.

Due to the requirement for nationwide WPS coverage, enlisting multiple carriers and multiple access technologies was critical. WPS is available in both the access technologies most widely available in the United States—Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA). The NCS continues to work with regional carriers for the provisioning of WPS. Full operational capability requirements for both GSM and CDMA are complete.

The provision of joint Industry Requirements (IR) provides a method for use of the Nation's cellular telecommunication networks by NS/EP personnel that will not hinder public use during emergency events by defining a standards-based priority queuing capability. As a result, a reasonable amount of capacity is always available for public use.

## WPS Benefits to the NS/EP Community

WPS is a significant emergency communications asset that has continuously proven to be effective for the NS/EP community. Just one of many examples was a comment in the aftermath of Hurricane Ike from Frost National Bank located in San Antonio, Texas, "...Because of GETS and WPS, Frost National Bank

employees were able to organize, direct, and communicate with assessment and recovery staff as well as existing employees in the area.”

Even though WPS is a much younger program than GETS, each year the program becomes stronger with the growth of more cellular companies, and expansion of the user base. Following the catastrophic tornadoes of March 2007, WPS benefited rescue workers and volunteers converging on the town of Enterprise, Alabama, when wireless networks were jammed. Prior to landfall for each hurricane, the NCS activated over 1,500 emergency cell phone requests for WPS services. During these hurricanes, the users reported a considerable improvement in the service compared to previous hurricane seasons.

WPS NS/EP Category	WPS NS/EP Users
Federal	62,171
State/Tribal	3,441
Local	8,484
Industry	10,210
Other NS/EP organizations	32
Total	84,338

Table 1. WPS User Breakdown

### FY 2008 Accomplishments and Improvements

In the past year, the WPS program continued to make significant progress in its outreach efforts to all levels of government and other qualified NS/EP industrial and non-profit organizations. As of September 15, 2008, there were 84,338 authorized WPS users—an 80-percent increase since September 17, 2007. Included within these numbers are 2,253 emergency activations that were processed and expedited after normal duty hours during critical FY 2008 events by the NCS Service Center personnel.

Additional WPS accomplishments during FY 2008 include:

- ▶ Signing a letter of understanding between Industry Canada and the NCS on WPS interoperability;
- ▶ Adding Alltel as a WPS CDMA carrier;

- ▶ Completing deployment of Phase 2/2A WPS CDMA in the Sprint PCS Nextel (CDMA) network;
- ▶ Completing development of the WPS CDMA Nortel/Motorola interoperability specification solution;
- ▶ Completing WPS CDMA interoperability specification interoperability testing with Verizon Wireless in time for WPS interoperability specification solution to be deployed to support the 2008 Presidential Conventions;
- ▶ Completing Network Service Acceptance Test with Cellcom for WPS CDMA full operational capability Phase 2A;
- ▶ Initiating a satellite priority service pilot program and installing the pilot program at the initial six sites; and
- ▶ Working with T-Mobile to expand WPS coverage in former SunCom areas not previously supported—North and South Carolina, Puerto Rico, and the U.S. Virgin Islands.

### Highlights and Status of Ongoing Activities

The NCS completed WPS CDMA development in two phases. In addition, Qualcomm completed its extension of a timer relevant for QSec-2700 WPS utilization in September 2008.



Sprint PCS will complete nationwide full operational capability implementation by December 2008. CDMA WPS development began in 2007 and was completed by July 2008 in time for deployment in the Verizon Wireless network for the 2008 Democratic and Republican National Conventions. Full interoperability





specification network deployment and WPS full operating capability is targeted for the fourth quarter of calendar year 2008 for Verizon Wireless, and April 2009 for Sprint PCS.

Many of the significant challenges facing WPS stem from technology upgrades, requiring the NCS to ensure continued availability of WPS capabilities as wireless carriers move to third generation (3G) wireless technologies. Universal Mobile Telecommunications System (UMTS) Directed Retry Handover (DRH) is an example of this effort to extend existing WPS to NS/EP community users utilizing 3G UMTS handsets. DRH solutions from a number of vendors, such as Nokia-Siemens Networks and Alcatel-Lucent, have completed product testing and are awaiting captive office testing. Additional vendors are expected to join the DRH effort in FY 2009.

### Partnership Activities

Like GETS, the NCS coordinates WPS use with the principle EOP groups and serves NS/EP users within the Federal, State, and local governments and other qualified NS/EP organizations. The NS/EP community supporting NS/EP mission requirements includes industry and non-government emergency response organizations plus industry owners and operators of critical infrastructures. Further, like GETS, WPS is an industry and government partnership dependent on the participation of the mobile equipment vendors and service providers. Current WPS industry partners include: Alcatel-Lucent, AT&T Mobility, Ericsson, Hewlett-Packard, Motorola, Nokia-Siemens Networks, Nortel, Qualcomm, Sprint Nextel, T-Mobile, and Verizon Wireless.

### NS/EP Priority Services in Next Generation Networks (NGN)

#### Background

Historically, NS/EP priority services such as GETS and WPS were specified, engineered, and implemented when the carriers based PSTN exclusively on circuit-switched technology. Today's PSTN is supplementing, and eventually replacing, circuit-switched equipment with the packet-based, Internet Protocol (IP) technologies that have supported IP data networks for some time. This transition to a packet-based technology dictates the evolution of GETS and WPS into the NGN. Using packet-switched technology, NGN GETS will provide priority NS/EP communications not only for voice band service, but also for broadband services such as video and data.

### Functional Description

The NCS expects the advent of priority voice for NGN to occur in a similar manner to that of GETS and WPS. A next generation voice user is expected to be able to use the current dialing methods for both GETS and WPS.

Priority data services will require new processes. End user data applications will be modified or new applications installed on equipment that will enable users to:

- ▶ Request priority treatment for an existing commercial service, such as instant messaging;
- ▶ Ascertain the status of the priority service; and
- ▶ Terminate priority treatment.

The initiation of priority treatment of services will require user authentication—whether done automatically through pre-subscription like the WPS model or manually by user entry of authorization information such as a personal identification number used in the GETS model.

### NGN Benefits to the NS/EP Community

NGN offers two key benefits to the NS/EP community. First, the evolution of today's networks from circuit to packet-switching will enable application of updates to the current GETS and WPS priority voice services in order to maintain or expand the current level of availability and reliability of priority voice services. Second, NGN capabilities will enable the addition of priority data and video applications, which are not available today, expanding NS/EP user mission capabilities in all critical situations. Thus, continued development of NGN priority services will ensure the NS/EP community can engage in priority voice, video, and data communications over the NGN.

### FY 2008 Accomplishments and Improvements

Working with service providers and equipment vendors, the NCS developed the voice service (Phase I) industry requirements for the IP Multimedia Subsystem (IMS) core network.

The NCS continues to collaborate with industry in the analysis of and experimentation with new technologies applicable to NS/EP services. NCS activities include, but are not limited to:



- ▶ Development of an IMS prototype lab to assess the feasibility of NS/EP video service;
- ▶ Continued detailed modeling and analysis of NS/EP NGN services;
- ▶ Participation in a priority video demonstration at the Verizon Industry Forum;
- ▶ Participation in the initiation of the Sprint NGN GETS prototype using IMS proof of concept architecture;
- ▶ Attendance at the 2008 Wireless CTIA Conference to evaluate advancements in wireless services and technology; and
- ▶ Evaluation of satellite services applicable to NGN priority services.

The NCS continues to support its cause in standards. During the period, the NCS:

- ▶ Was elected as Vice Chair of the MultiService Forum (MSF) Technical Committee;
- ▶ Received the MSF's "Award of Excellence";
- ▶ Participated in the ATIS Workshop; and
- ▶ Provided an Internet Engineering Task Force (IETF) draft contribution on Session Initiation Protocol (SIP) overload control.

The NCS described its NGN activities and obtained feedback from the NS/EP community at the two-day GETS/WPS Team Forum held May 19-21, 2008, in Glen Allen, Virginia. The NCS briefed the community of its recent access IR activities and sought feedback from the community on many topics.

### Highlights and Status of Ongoing Activities

The NCS is currently working with industry to:

- ▶ Develop the descriptions for next generation priority services such as video conferencing, Web browsing, and email;
- ▶ Develop the industry requirements for NGN service access requirements for six access technologies; and

- ▶ Update the IMS core network requirements to align with the forthcoming access requirements.

### Partnership Activities

The NCS is actively participating in Standards Development Organizations (SDO) and fora, coupling its industry liaisons and IR processes with initiatives to ensure that the appropriate standards include NS/EP NGN needs.

The NCS continues to participate in the activities of the MSF, including the planning and preparation for the Global MSF Interoperability testing event (GMI 2008), scheduled for FY 2009. The NCS and industry partners plan to demonstrate proof of concept priority capabilities that address NS/EP NGN needs. The NCS plans to demonstrate priority features such as video teleconferencing, dynamic priority, media packet priority, and anonymity in the IP environment, security across the network-network interface, priority 800 calling, and priority three-way calling. The NCS will also demonstrate these features on a global scale using commercially available NGN equipment.

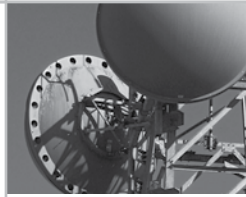
The NCS presented industry with two papers:

- ▶ "Global Interoperability of NS/EP Telecommunications Services," Institute of Electrical and Electronic Engineers (IEEE) 3rd Annual Secure Communications Conference (SecureComm2007), Nice, France, September 17-20, 2007; and
- ▶ "National Security and Emergency Preparedness Multimedia Service in a Congested Network," IEEE International Symposium on Broadband Multimedia Systems, Las Vegas, Nevada, March 31-April 2, 2008.

The NCS will continue joint development of NS/EP solutions with industry partners—an approach used during the development of the GETS and WPS programs. This ensures the provision of priority services to users with NS/EP mission requirements.

### NS/EP Standards Development

Presidential Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, directs NCS consideration of evolving national and international standards with respect to NS/EP telecommunications, and OMB Circular A-119, *Federal Participation in the Development and use of Voluntary Consensus Standards*





and in *Conformity Assessment Activities*, calls for Government to adapt the products of commercial/industry standards committees and to participate in their development. The NS/EP Standards Team personnel work with a number of national and international telecommunications industry standards organizations to ensure that everyone uses evolving commercial standards as a basis for NS/EP telecommunications.

Emergency Telecommunications Services (ETS) include ongoing NGN standards development initiatives encompassing prime functionalities of: signaling, access, management, transport, interoperability, mobility, and their associated architectures.

Engineers designed traditional NS/EP telecommunications services around the circuit-switched infrastructure of the PSTN; however, public networks are now merging with packet-switched infrastructures and evolving into converged NGN. As this evolution continues to mature, commercial standards stemming from technologies based on packet-switching, such as IP-based networks, will guide future priority telecommunications services.

The IEEE 802.16 Working Group is developing Project 802.16m—System Description Document. The NCS is participating in the technical development of this standard to ensure that the air interface for WiMAX networks supports priority access.

The NCS has several work items currently underway in the Third Generation Partnership Project (3GPP) and the Third Generation Partnership Project 2 (3GPP2). TS 22.153: “Multimedia Priority Service stage 1 Description for the GSM/UMTS-based Systems” is the 3GPP work item and S.R0117-0 v1.0: “Multimedia Priority Service for MMD-based Networks—Stage 1 requirements for CDMA-based Systems” is the 3GPP2 work item. The objective of these activities is to develop Priority Services Standards/Specifications for next generation wireless networks.

The NCS-led IMS access IR effort is tightly coupled with the ongoing work activity in both 3GPP and 3GPP2. The output from the IMS IR is brought into 3GPP and 3GPP2 as contributions in order to ensure that the developing specifications meet the NCS NS/EP requirements. Two areas of interest to the NCS are 3GPP2 projects X.P0058 “WiMAX-HRPD Intw Core Network Aspects” and X.P0057 “UTRAN-HRPD Interworking—Core Network Aspects,” which are the foundation for the evolving 4th Generation All-IP wireless networks.

The NS/EP Standards Team provides direct support to the U.S. Department of State by chairing the International Telecommunications Advisory Committee Study Group ‘B’ along with serving as senior Government advisors and leaders, such as heads of delegations, to a variety of international and national meetings on next generation telecommunications developments. In addition to this study group, team members participate in the work of various commercial/industry standards development organizations including:

- ▶ ATIS;
- ▶ Telecommunications Industry Association (TIA);
- ▶ International Telecommunication Union, Telecommunication Standardization Sector (ITU-T);
- ▶ IETF;
- ▶ TeleManagement Forum (TMF);
- ▶ 3GPP;
- ▶ 3GPP2; and
- ▶ IEEE.

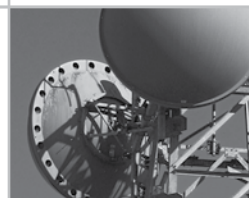
In concert with the above listed organizations, team member participation includes:

- ▶ Conducting studies, performing analyses, sponsoring industry/academic research, and developing new technologies for potential NS/EP applications;
- ▶ Firmly establishing NS/EP technical requirements in standards work programs, in cooperation with industry and academia;
- ▶ Developing and providing detailed technical proposals—such as NS/EP technical contributions—within industry standards programs, encouraging industry participants in these programs to make technical proposals to augment NCS proposals;
- ▶ Encouraging and promoting independent testing and implementations of proposed technical solutions; and
- ▶ Participating in the development of contemporary telecommunications industry acquisition tools, such as service level agreements (SLA) and associated application notes for IP-based services, to better specify criteria for availability, reliability,

and quality performance of delivered NS/EP telecommunication services.

Accomplishments in FY 2008 include:

- ▶ ATIS
  - ATIS-1000023[1] [pre-pub] ETS Phase 1 Network Element;
  - ATIS-0100009 Standards Support for ETS;
  - ATIS-1000020 ETS Packet Priority For IP Network to Network Interface (NNI) Interfaces-Requirements For a Separate Expedited Forwarding Mechanism;
  - ITU-T Standards Developments;
  - (ITU-T SG 16) Supplement 9 to ITU-T H-Series Recommendations—Operation of H.248 with H.225, Session Initiation Protocol (SIP), and ISDN User Part (ISUP) in Support of ETS/International Emergency Preference Scheme (IEPS) (approved May 2008);
  - Supplement 57 to the ITU-T Q-series—Signalling Requirements to Support the ETS in IP Networks;
  - (ITU-T SG 13) 2008, Progressed the development of new proposed Recommendation Y.NGN-ET-TECH (Next Generation Networks—Emergency Telecommunications—Technical Considerations) for approval in 2008; and
  - (ITU-T SG 9) 2008, progressed the development of draft Recommendation J.pref on technical specifications to enable preferential (GETS-like) communications in the current suite of Next Generation IP Cablecom networks that industry is now deploying.
- ▶ Internet Engineering Task Force Request For Comments (RFC)
  - Achieved approval of new RFC 4958 on A Framework for Supporting Emergency Telecommunication Service within a Single Administrative Domain. This new RFC and other ETS associated completed RFC in previous years, are now included as background and guidance for RFC 4542, *Implementing an ETS for Real-Time Services in the Internet Protocol suite*;
- Progressed draft RFCs:
  - DiffServ Code Point draft-IETF Capacity-Admitted Traffic;
  - Draft-IETF Quality of Service Attributes for Diameter; and
  - Draft-IETF Resource Reservation Protocol (RSVP) Extensions for Emergency Service.
- ▶ Approved RFC 5115 Telephony Routing over IP (TRIP) Attribute for Resource Priority
  - Emergency Extensions to the RSVP
- 3rd Generation Partnership Project;
  - 3GPP TS 22.153 (Release 8) aligned with the NGN GETS IMS Core Network IR output;
  - 3GPP TS 22.153 (Release 9) updated to include support for GETS-AN and GETS-NT invocations;
  - 3GPP TS 22.153 (Release 9) Stage 1 Multimedia priority Service approved; and
  - Initiated work to address Multimedia priority Service Stage 2 (call flow) and Stage 3 (interface) aspects.
- 3rd Generation Partnership Project 2
  - S.R0131-0 v1.0 IP Multimedia System Centralized Services (ICS) Stage 1 Requirements updated to include support for Priority Services requirements (S.R0117-0 v1.0). ICS allows IMS-based services to be delivered to users regardless of the attached access network type.
- IEEE
  - Air Interface Priority Access;
  - Initial draft: Prioritized Quality of Service (QoS) Framework—MAC Layer Connection Establishment and Maintenance; and
  - Initial draft: Prioritized QoS Framework—MAC Layer Network Entry.





### Modeling, Analysis, and Technology Assessment

As directed by E.O. 12472, the NCS developed modeling and analysis techniques and applications to “Conduct technical studies or analyses. . .for the purpose of identifying. . .improved approaches which may assist Federal entities in fulfilling national security or emergency preparedness telecommunications objectives.”

### Network Design and Analysis Capability (NDAC)

Due to the NS/EP community’s heavy reliance on the PSN, the Network Design and Analysis Capability (NDAC) was developed to analyze current U.S. networks and technologies, and to evaluate the need for additional capabilities. The NCS has invested over 20 years in establishing strong working relationships with commercial carriers and Government departments and agencies, and developing modeling tool sets, methodologies, and unique databases that include proprietary data from the major carriers. The NDAC provides a comprehensive modeling and analysis capability and the ability to model the impact of a wide variety of scenarios, such as:

- ▶ What impact would a pandemic flu have on the telecommunications infrastructure?
- ▶ What impact will the convergence of traditional circuit-switched networks with packet-switched/IP-based networks have on NS/EP requirements?

Tools within the NDAC suite include the following:

The Infrastructure Mapping Tool (IMT) is a Geographical Information System (GIS), situational awareness tool used for pre-event planning and analysis, as well as post-event response. IMT provides analysis of critical infrastructures for incident management, decision support, and status tracking. When an event occurs that has the potential to disrupt network infrastructures, IMT can create detailed infrastructure analyses for specific geographic areas of concern. IMT can layer near real-time data over infrastructure data pulled from numerous proprietary and government databases. The results can define the scope of impact, create specific impact area views, run initial assessment reports, create up-to-date visualizations of asset status, and conduct telecommunications impact analyses relevant to specific users, businesses, and government agencies.

The Communications Network Analysis Tool (CNAT), originally developed for the Department of Defense (DOD) Mission Assurance Division (MAD), is now shared with the NCS to complement and extend its NDAC tool suite. CNAT provides a communications analysis capability by querying Central Location On-line Entry System (CLONES) data and displaying the results on a map. Analysts can perform the basic functions of CNAT through a GIS interface to support telecommunications queries. Users can import query results to various applications for presentation to key decision makers to aid in determining impact assessments on a timely basis.



An increasing number of Government NS/EP users are utilizing Internet services; consequently, models of the logical and physical infrastructures of the Internet are now required to support NS/EP analyses. With the ongoing NDAC expansion to include packet-switched networks, the NCS developed an Internet Analysis Tool (IAT) to capture physical and logical interdependencies between Internet Service Providers (ISP). The NCS is expanding the tool into an Internet Analysis Capability (IAC) that will provide both architectural and traffic perspectives and will incorporate commercial off-the-shelf (COTS) products that add the capability to determine the reliance of NS/EP services on the assets and configuration of the Internet’s infrastructure—and provide situational awareness information. This expanded capability enables the NCS to:

- ▶ Identify network anomalies and determine how they impact communities of interest;
- ▶ Characterize the relationships and interdependencies between ISPs and other infrastructure providers;
- ▶ Integrate and correlate internal and external routing, inventory, and activity data, and scale to include any computer network-related data source;
- ▶ Access and collect global Internet routing data that provides, at a minimum, 90-percent coverage of usable Internet space;
- ▶ Collect and visualize netflow data for malicious activity investigation;
- ▶ Visualize global and local networks with Google Earth-like functionality; and
- ▶ Provide both an interface for operational analysts and a management interface for operations center managers.

#### **Traffic Analysis of Critical Federal Telecommunications Infrastructures**

The NCS has developed an analysis tool that uses FTS2001 and Networx data to interactively view an agency's traffic inventory and perform critical infrastructure/sensitivity analysis on the impact to the traffic if a telecommunications facility is disabled. Critical infrastructure analyses occurred for 11 NCS member agencies, including GSA, NASA, Department of Transportation, National Telecommunications and Information Administration (NTIA), U.S. Department of Agriculture, Department of Health and Human Services, Nuclear Regulatory Commission, Department of State, Department of Energy, Department of the Interior, and DHS. Analyses include graphical mapping to view the impact of a disabled point of presence (POP) or wire center based on Government traffic. The NCS provides diversity recommendations for agency locations to avoid losing telecommunications service due to a POP and/or wire center outage.

#### **Risk Assessment Methodology**

The NCS partnered with industry to lead the National Sector Risk Assessment (NSRA) for communications in support of the Communications Sector Specific Plan (CSSP). Completed actions include:

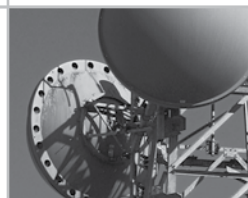
- ▶ Co-led the development of the CSSP Implementation Working Group with industry, formed to address the risk milestones outlined in the CSSP;
- ▶ Coordinated several working group meetings to discuss the architectural framework and methodology for the NSRA;
- ▶ Outlined examples and working group starting points for threats, vulnerabilities, and consequences;
- ▶ Developed concepts for qualitative risk assessment methodologies that address threat, vulnerability, and consequence; and
- ▶ Cooperated with industry to develop and obtain working group agreement on a risk methodology framework.

In addition to NSRA-related efforts, the NCS supports cross-sector dependency analyses as outlined by the CSSP. A qualitative detailed risk assessment framework, including an example implementation of the framework, instigates the development of a capability to identify:

- ▶ Consequences, vulnerabilities, and threats to the communications architecture;
- ▶ Architecture elements and functions that could be nationally critical, as defined by Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization, and Protection*;
- ▶ Specific assets related to an architecture element or function deemed to be at high risk; and
- ▶ Protective measures to mitigate risk.

#### **Priority Services Modeling (PSM)**

The convergence of the circuit-switched architecture of the PSTN with the packet-switched technologies of the Internet is changing the communications infrastructure that formed the basis for NCS programs and analyses. As the infrastructure changes, NDAC tools and methodologies must evolve to effectively analyze the implications of NS/EP services transitioning to these next generation network architectures. The NDAC Priority Services Modeling (PSM) team must address multiple new questions introduced by the evolution of traditional GETS/WPS services to NGN architectures, such as:







- ▶ Will these new architectures be able to support viable communications at 10x overload and with up to 70 percent infrastructure damage?
- ▶ How will industry's move toward IMS-based solutions affect the performance and reliability of current NS/EP services?
- ▶ How will the NGN provide priority e-mail, video teleconferencing, and other multimedia services?

The NDAC responded to these emerging challenges by modeling the effectiveness of various priority service features—with respect to network and application performance—under various damage and congestion scenarios. The results of these modeling efforts have been:

- ▶ Incorporated into the GETS/WPS programs' IR process;
- ▶ Briefed at various CS&C conferences, such as the GETS Team Forum; and
- ▶ Submitted as a draft document to the IETF.

Given that service providers' technologies, architectures, and protocols are in a constant state of flux, the NDAC plans to continue its priority services modeling work throughout the upcoming year and produce modeling studies to aid the decision-making process of the GETS and WPS programs. The NCS is currently working on two studies/reports: *Survivability Dependence on Internetwork Routing Policies and Interface Throttling to Prevent Denial of Service*. The results of these and other modeling studies will quantify the effectiveness of proposed priority service mechanisms and feed policy and budgetary decisions related to both the GETS and WPS programs.

#### Committee on Foreign Investment in the U.S. (CFIUS)

The NCS is an active Committee on Foreign Investment in the United States (CFIUS) participant, with specific objectives to manage the critical infrastructure risk caused by globalization of the telecommunications sector and respond to the unique policy challenges created as the United States



continues to encourage foreign investment while balancing security priorities. This work involves conducting critical infrastructure analysis to identify key telecommunications assets and associated vulnerabilities, and providing technical and policy analyses to increase the level of transparency in commercial mergers and acquisitions.

#### DHS OneNet Integration Support

When 22 agencies were brought together to create DHS, an incongruent myriad of information technology (IT) systems resulted. The DHS Chief Information Officer's (CIO) challenge is to integrate these systems into DHS OneNet under GSA's new Networx contract. Throughout this fiscal year, the DHS CIO has opted to use the NCS' demonstrated network modeling proficiency, tools, and data to support this effort.

#### Technology Assessment and Data Analysis Cell

The NCS developed a fully accredited facility to provide the capability to:

- ▶ **Evaluate Contract Deliverables**—The Technology Assessment and Data Analysis Cell (TADAC) provides a facility to evaluate the hardware and/or software deliverables of some contracts for acceptance purposes;
- ▶ **Evaluate Products**—The TADAC provides a platform to research, identify, and evaluate off-the-shelf products (COTS and Government off-the shelf [GOTS]) that may satisfy specific NS/EP requirements, often obviating development contracts;
- ▶ **Host Applications & Databases**—The TADAC provides the host environment for several applications and associated databases developed specifically to ensure survivable and robust communications in support of NS/EP requirements. These applications include the NDAC—a set of tools, data sets, and methodologies that enable modeling and analysis of the PSN;
- ▶ **Provide Component-Level Simulation**—Although the NDAC provides a macro view of network behavior, it lacks the ability to adequately simulate the behavior and interaction of individual pieces of software and hardware. The TADAC provides this type of simulation;

- ▶ **Participate in Community Research Projects**—The TADAC enables the NCS to move beyond its role as a patron or sponsor of research, to become an actual participant. Internet community projects provide an excellent opportunity to enhance engineers' and computer scientists' expertise in critical areas and increase the respect and recognition of the NCS within research and development circles; and
- ▶ **Training**—The TADAC provides an environment to support ongoing hands-on technical training, an alternative to expensive vendor-provided training.

The TADAC contains two networks: the eXperimental Testbed Environment (XTE) and the Technology Assessment Network (TAN), which are described below.

#### **eXperimental Testbed Environment**

The XTE provides the ability to emulate a scaled-down version of the Internet, converged network service provider networks, and enterprise networks. Operators simulate severe congestion on both the network and NGN end systems, and test and validate that emergency telecommunications services work properly from end-to-end using call load generators, traffic generators, and associated customized call processing systems. The XTE is a distributed test environment consisting of:

- ▶ Network devices (routers and switches) simulating an ISP's backbone/core and access network;
- ▶ Security devices (authentication systems, firewalls, session border controllers, and intrusion detection capabilities) to protect network assets by enabling access control and by detecting and responding to simulated threats;
- ▶ Hosts and servers enabling the invocation and termination of NGN services and priority services;
- ▶ Test and analysis equipment to generate voice, video, and data traffic and to gather results of the effects of congestion on NGN services and service elements;
- ▶ Voice over Internet Protocol (VoIP) telephones and systems to represent a VoIP service provider's service infrastructure; and
- ▶ Video endpoints and systems to access scaled-down IMS core NGN network service platforms with NS/EP functionality.

#### **Technology Assessment Network**

The TAN consists of a suite of equipment enabling PSN analyses in support of the Federal Emergency Management Agency's (FEMA) Emergency Support Function 2-Communications (ESF #2) function. Primarily set up as a "surge" capability, the NDAC portion of the TAN replicates the modeling and analysis capability generally provided by a variety of contractors, except that certain proprietary data sets are not available. Additionally, the TAN provides the capability to evaluate cutting edge technology without jeopardizing existing development or production systems. This includes COTS/GOTS application evaluation and testing with respect to compatibility and interoperability, load stress, security features, and vulnerability identification. The TAN also hosts applications, databases and web-based tools; provides component-level network simulation; enables participation in community research projects; and provides a highly advanced training platform.

#### **Advanced Technology Group**

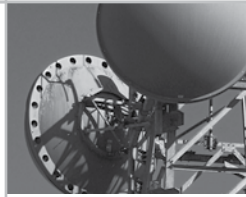
The NCS Advanced Technology Group (ATG) leads the effort in identifying vulnerabilities of legacy and emerging communications systems to Telecommunications Electromagnetic Disruptive Effects (TEDE); ATG also focuses on identifying vulnerabilities or opportunities in communications systems to benefit NS/EP. The ATG supports multi-agency efforts to improve the national emergency communications infrastructure; the following paragraphs address support efforts in detail.

#### **Telecommunication Electromagnetic Disruptive Effects**

Title 5 of the Code of Federal Regulations (C.F.R.), Part 215, assigns the Executive Agent of the NCS as the Federal Government's focal point for electromagnetic pulse (EMP) technical data and studies concerning telecommunications. The NCS defines TEDE as encompassing EMP, Magneto Hydro Dynamics (MHD), High Power Microwave (HPM), Directed Energy Systems, High Radiation Environments, solar flares, and the effects of lightning.

The ATG continues to coordinate and conduct studies in the following topical areas:

- ▶ Susceptibility of the telecommunications infrastructure to EMP;
- ▶ Approaches to telecommunications systems protection from TEDE;





- ▶ Hardening essential communications systems, continued surveillance, and maintenance;
- ▶ Protection for new communications technologies and systems; and
- ▶ Affordability of EMP protection.

TEDE susceptibility tests of the telecommunications infrastructure include:

- ▶ PSTN switching systems and infrastructure;
- ▶ Terrestrial/satellite transmission and power systems;
- ▶ Equipment level tests and network level modeling;
- ▶ Partnered with Congressional “Live Fire” high power microwave vulnerability tests of Supervisory Control and Data Acquisition systems, PSTN switching systems, local area networks and computer systems;
- ▶ Disruption of fiber-optic telecommunication links due to secondary effects associated with high energy illumination;
- ▶ Internet systems vulnerability tests; and
- ▶ Aviation Transportation communications systems vulnerability tests.

These studies are performed in partnership with the Air Force Research laboratories and private industry. The NCS shares results confidentially with participating companies, who use these results to modify their system components to be TEDE-resistant within known parameters. Companies with systems that provide relevant systems in the telecommunication infrastructure are encouraged to participate in these collaborative efforts. The NCS continues to represent DHS as a guest subject matter expert to the Congressional EMP Commission.

### Emergency Communications and Evolving Technologies Studies

The ATG evaluates the ability of different modalities of communications to support NS/EP purposes; including both satellite and advanced terrestrial systems. The ATG also continues to support upper management as the subject matter experts in sudden advanced technologies issues related to communications,

including but not limited to, positioning, navigation, and timing (PNT), satellite communications, and wireless and landline networks.

The ATG identified vulnerabilities to a wide array of assets, including: airborne passenger information networks, undersea cable communications, telecommunications power dependencies, timing issues of networks, broadband cellular, IP television implications to telecommunications, and multimedia traffic in cellular networks and PSN.

These studies support ongoing governmental and industry working groups efforts to maintain robust communication networks for NS/EP purposes.

### Warning Alert Response Network Act

Americans increasingly rely on wireless telecommunications services and devices to receive critical, time-sensitive information anywhere, anytime. To ensure the ability of the Nation’s wireless carriers to transmit timely and accurate alerts, warnings, and critical information to the cell phones and other mobile devices, an FCC Commercial Mobile Service Alert Advisory Committee (CMSAAC) developed requirements through the formation of working groups comprised of industry and Government personnel.

ATG staff participated in development of the Cellular Mobile Alert Service (CMAS) requirements and were members of the Alert Interface Group (AIG) chartered under the CMSAAC to develop CMAS interface requirements. As a result of the CMSAAC team effort, the FCC adopted a First R&O in support of the *Warning Alert Response Network (WARN) Act* (Action by the Commission, April 9, 2008, by Commercial Mobile Alert Service First Report and Order [FCC 08-99]).

### Transformational Communications Architecture

The ATG is supporting the development of the DHS contribution to the National Security Space Office (NSSO) Transformational Communications Architecture (TCA). The TCA is an ongoing space transport-level architecture that works in concert with the Global Information Grid (GIG) to help synchronize multiple acquisitions; promote standards and interoperability; deliver time-phased capability in an evolutionary approach; and support information architecture concepts that enable critical information sharing needs. The TCA involves: SATCOM satellites of DOD, the United States Intelligence Community, NASA, and DHS-leased commercial

mobile and fixed satellite services; SATCOM Terminals; Terrestrial Infrastructure (Teleports and Gateways); and Network Management and Information Assurance to control the space assets and entry into the ground infrastructure.

### Communications Dependency on Electric Power Working Group

The heavy reliance of the communications infrastructure on electric power has come to the forefront of attention in the wake of national emergencies such as the 2003 Northeast blackout and Hurricanes Katrina and Rita in 2005. In December 2006, the President's National Security Telecommunications Advisory Committee (NSTAC) published its *Report to the President on Telecommunications and Electric Power Interdependencies, The Implication of Long-Term Outages (LTO)*.



The Ghent Power Plant, in Ghent, Kentucky, as viewed from a NOAA hurricane hunter aircraft in 1999.

As such, the critical imperative to ensure NS/EP communications necessitates that the Federal Government conduct studies to analyze the scope and nature of those dependencies in both short-term and long-term outage situations, and the vulnerabilities to NS/EP communications that they create.

In August 2007, the NCS Committee of Principals (COP) voted to establish the Communications Dependency on Electric Power Working Group (CDEP WG) to examine issues raised by and relating to the NSTAC Report to the President on *Telecommunications and Electric Power Interdependencies, The Implication of LTOs*, and to work in concert with the private sector to address the full set of recommendations issued by the NSTAC. The ATG participated in CDEP WG efforts to study the LTO recommendations of the NSTAC to the President. Moreover, the ATG helped plan the CDEP WG LTO Workshop; participated in investigating government science and technology research efforts; and assisted in investigating LTO communications power dependencies.

### NCS Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, and Continuity Communications Architecture

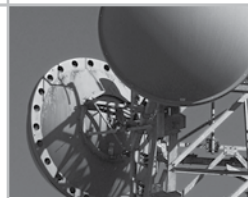
Two directives outline mandate for Executive Branch continuity communications:

- ▶ National Security Presidential Directive 51/Homeland Security President Directive 20 (NSPD-51/HSPD-20), *National Continuity Policy*, May 9, 2007; and
- ▶ NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, July 25, 2007.

National Continuity Policy in NSPD-51/HSPD-20 sets forth a new vision to ensure the continuity of government. The purpose of the directive is to establish and maintain a comprehensive and effective continuity capability composed of Continuity of Operations (COOP) and Continuity of Government (COG) programs in order to ensure preservation of government under the U.S. Constitution and the continuing performance of National Essential Functions (NEF) under all conditions. The four key areas addressed include department and agency leadership; staff; communications; and facilities.

### Continuity Communications Architecture

The DHS Secretary, as Executive Agent of the NCS, is responsible for developing, implementing, and maintaining a comprehensive Continuity







Communications Architecture (CCA). The CCA is an integrated, comprehensive, interoperable framework of continuity communications requirements, based upon the department and agency communications needs to perform their primary mission essential functions (PMEF) in support of NEFs, during both routine and continuity conditions. The CCA utilizes voice, data, and video solutions, as appropriate, to ensure communications and business systems, including hardware and software for continuity operations, mirroring those used in day-to-day business to assist continuity leadership and staff in a seamless transition to crisis operations.



Power lines in Houma, Louisiana, become entangled in trees from Hurricane Gustav's powerful winds and rain. (Photo by Jacinta Quesada/FEMA)

Based upon technical requirements from OSTP, the NCS will develop, implement, and maintain a CCA. The CCA shall include the minimum requirements necessary to finalize selection of a secure communications system by DOD.

### FY 2008 Accomplishments

In the past year, the NCS has made significant progress in developing analytical capabilities to collect and analyze department and agency PMEFs and Mission Essential Functions (MEF) data and communication needs. Capabilities and accomplishments include:

- ▶ Developed MEF/PMEF data capture tools to facilitate MEF/PMEF data entry;
- ▶ Established Top Secret-level repository for analysis of MEF and PMEF data;
- ▶ Developed analytical methods and tools to identify inter-agency relationships including communications capability gaps; and
- ▶ Supported DHS, DOD, and Intelligence Community (such as the National Reconnaissance Office [NRO], and Federal Bureau of Investigation [FBI]) for PMEF/MEF data collection and aggregation activities.

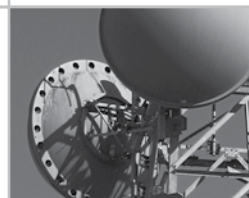
### FY 2009 Challenges

Ensure a seamless transition from the PMEF/MEF validation phase to the CCA development phase. Issues include PMEF/MEF realignment, communications data collection, and interdependency gap analyses activities within the timelines identified.

### NCS Directive 3-10, Minimum Requirements for Continuity Communications Capabilities

NSPD-51/HSPD-20 requires that all departments and agencies incorporate continuity requirements into daily operations. NCS Directive 3-10 establishes the minimum communications requirements (non-secure and voice, data and video, mobile/in-transit backup communications, and priority access and restoration services) for Federal department and agency headquarters and continuity alternate operating facilities. The intent is to establish a Federal inter-agency communications baseline of minimum requirements that supports the execution of PMEFs in support to NEFs and enable senior leadership to collaborate, develop policy recommendations, and act under all circumstances. In addition, NCS Directive 3-10 requires the departments and agencies to report compliance quarterly and to participate in monthly testing of the operational capabilities at their headquarters and all alternate operating facilities.





The NCS manager publishes supporting implementation guidance; conducts testing; develops a quarterly compliance report of the communications requirements; and annually develops for consideration by the NCS COP and the Executive Agent, DHS, recommended updates to the NCS Directive 3-10. A COOP Communications Managers Group (CCMG), established in December 2004 and co-chaired by the Manager, NCS, and FEMA, provides a classified forum to address department and agency COOP communications issues, including NCS Directive 3-10 implementation planning, compliance testing and reporting, and interoperability.

In the past year, the NCS has made significant progress supporting the departments and agencies in implementation activities by publishing implementation guidance, including:

- ▶ NCS Manual 3-10-1, *Guidance for Implementing NCS Directive 3-10*; and
- ▶ NCS Handbook 3-10-1, *Guidance for Improving Route Diversity within Local Access Networks*.

The NCS is currently in the process of releasing draft revisions to NCS Directive 3-10 for review by the COP.

Since January 2008, the NCS has been conducting NCS Directive 3-10 mandated communications testing and released the initial NCS Directive 3-10 compliance report in June 2008.

### FY 2009 Challenges

- ▶ **Continuity communications requirements updates**—Developing updates to the directive based upon department and agency communication mission needs, and policy, legal, and regulatory mandates;
- ▶ **Compliance testing and reporting**—Evolving NCS Directive 3-10 testing program from voluntary to mandatory, maximizing department and agency test and reporting participation; and
- ▶ **Identification of funding stream and Congressional support**—Departments and agencies are currently funding internally for NCS Directive 3-10 compliance through FY 2009.

### Looking Ahead

The ATG plans to continue TEDE vulnerability assessments of the NGN and track, evaluate, and advise management of ongoing changes to satellite communications with the advent of, such developments as, hybrid communications technologies and industry implementation plans that would effect NS/EP communications. The ATG will continue to participate or lead Federal Government efforts to improve minimum communications and continuity of communications architectures in support of NEFs and NS/EP communications.

### Critical Infrastructure Protection Branch

The Critical Infrastructure Protection (CIP) Branch, through its valued industry-Government partnerships, ensures the availability of critical NS/EP communications services across the full spectrum of emergencies. Emergencies include, but are not limited to, conventional and terrorist attacks against the United States, natural and man-made disasters, and other crises.

### Organizational Structure

The CIP Branch is organized around its role to prepare for and respond to incidents that impact NS/EP communications. After the devastating 2005 hurricane season, the branch re-organized to include the following teams:

- ▶ **Operations Team**—Coordinates and manages emergency response, operations, and information-sharing activities among the communications industry, Government, and international partners;
- ▶ **Contingency Planning (CP) Team**—Develops and implements emergency response doctrines and operational plans;
- ▶ **Operational Analysis (OA) Team**—Provides near real-time analytical assessments of the communications infrastructure; and
- ▶ **Training and Exercise (TE) Team**—Develops a cadre of knowledgeable and skilled emergency response personnel.



## Operations Team

The Operations Team is responsible for emergency response, operations, analysis, and information-sharing activities with industry, Government, and international partners. The team manages day-to-day operations of the National Coordinating Center (NCC), the Communications Information Sharing and Analysis Center (COMM ISAC), and several operational programs to include SHARED RESOURCES (SHARES) High Frequency (HF) Radio and Telecommunications Service Priority (TSP).

## National Coordinating Center for Telecommunications

The NCC, as an industry-Government collaborative body, is the primary mechanism within the NCS for fulfilling its emergency response role. The NCC's mission is "to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications service or facilities under all conditions, crises or emergencies." With 49 industry participants and 24 Federal Government agencies represented at the NCC, having both public/private industry working in close proximity to one another is the mechanism that ensures the success of the NCS and NCC missions.

As the operational arm of the NCS, the NCC Watch is a 24x7 watch and analysis operation center. Co-located with the United States Computer Emergency Readiness Team (US-CERT) and staffed by senior-level information analysts, the NCC Watch is the focal point for all NCS emergency response operations. During a response, Government personnel communicate NS/EP requirement priorities to industry, and industry representatives provide the Government with expertise, resources, situational awareness, and status of the telecommunications infrastructure.

## Major NCC Activities in 2008

- ▶ Completed the NCC's move from the Defense Information Systems Agency (DISA) South Courthouse Road facility to the DHS Glebe Road complex in October 2007. The move co-located the NCC Watch with the National Cyber Security Division (NCS) US-CERT, allowing the two operations to leverage existing synergies and converging aspects of the telecommunications and information technology sectors.
- ▶ Coordinated with FEMA to establish a co-primary agency relationship for ESF #2 incident responses. This shared role allows each agency to leverage its resources and best utilize its inherent strengths. FEMA leverages its extensive tactical communications resources and well-established regional presence, while the NCS provides the benefits of the NCC with its long-standing support and interaction with the communications infrastructure owners and essential service providers. When activated, ESF #2 personnel establish the Disaster Emergency Communications (DEC) Branch within the operations section at the Joint Field Office, along with providing liaisons to other Federal response organizations at the regional and national levels.
- ▶ Maintained situational awareness and proactively engaged its ESF #2 and industry partners for areas impacted by: California wildfires, Middle East cable cuts, New York City Global Positioning System (GPS) interference issues, Midwest floods, and the Gulf Coast hurricanes.
- ▶ Actively tracked, analyzed, and assessed approaching storms to include Hurricanes Bertha, Dolly, Gustav, Hanna, Ike, and Kyle, and Tropical Storms Arthur, Cristobal, Edouard, Fay, Josephine, and Laura. Four of the 12 named storms made United States landfall in 2008 as Category 1 hurricanes or higher, which resulted in cross sector critical infrastructure impacts and major flooding.
- ▶ Conducted daily conference calls with its industry-Government partners during the 2008 hurricane season to coordinate pre- and post-landfall staging, access, security, and fuel provision response activities in coordination with ESF #2 support elements and industry liaisons.
- ▶ During the 2008 hurricane season, the NCS, in coordination with the FCC, activated the Disaster Information Reporting System (DIRS) for Tropical Storm Fay and Hurricanes Gustav and Ike. DIRS is an online system that allows communications providers (public safety, television, radio, cable, cellular, and telephone) to report the status of their infrastructure within a disaster area. The information collected provides situational awareness and supports the prioritization of NS/EP restoration requirements.



A number of houses remain standing next to pilings where neighboring houses once stood in Bolivar Peninsula, Texas, on September 24, 2008. The peninsula has pockets of complete devastation from Hurricane Ike. (Photo by Jocelyn Augustino/FEMA)

- ▶ Administered the DHS Emergency Notification System (ENS) as a means of notifying both industry and government personnel during emergent/time-sensitive events. Over the last year, the NCS used ENS for both real-world support (such as the California wildfires, and Hurricanes Dolly and Gustav), and for training and exercise events such as Top Officials (TOPOFF) 4, Cyberstorm II, and National Level Exercise (NLE) 2-08. The DHS ENS system is the prototypical notification system that has proven to be cost-effective, efficient, and actionable for the NCS and its industry-Government partners.
- ▶ Participated in three NLEs to include TOPOFF 4, Cyberstorm II, and National Level Exercise 2-08.
- ▶ Participated in the annual ESF #2 Winter Training Conference held at SAIC facilities in McLean, Virginia. The ESF #2 Winter Training Conference trains members from ESF #2 support elements (including GSA, FCC, and NTIA), as well as industry representatives to address new policies for ESF #2 organization and operations. Participants also took part in a practical exercise on information management within ESF #2.
- ▶ Hosted the first NCC Day in April 2008, at the Glebe Road facility. NCC Day was an opportunity to welcome and indoctrinate both new and existing NCC industry partners representing the COMM ISAC on the roles and responsibilities of

DHS, NCS, NCC, and the unique role of the COMM ISAC in NS/EP disaster response.

- ▶ Developed and contributed to a number of policy and strategic documents to include the DHS NPPD Pandemic Flu Plan, the DHS CS&C Strategic Framework for International Engagement, and the Office of Emergency Communications (OEC) National Emergency Communications Plan (NECP).
- ▶ Expanded its COMM ISAC membership to include wireline and satellite representatives.

### Communications Information Sharing and Analysis Center

In 2000, the National Coordinator for Security, Infrastructure Protection and Counterterrorism designated the NCC as the ISAC for the communications sector per the guidance of the 1998 Presidential Decision Directive (PDD) 63, *Protecting America's Critical Infrastructures*. This directive encouraged the private sector to establish ISACs to "serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information." As part of the ISAC mission, information regarding threats, vulnerabilities, intrusions, and anomalies is collected from the communications industry, Government, and other sources and then analyzed with the goal of averting or mitigating impacts on the communications infrastructure.



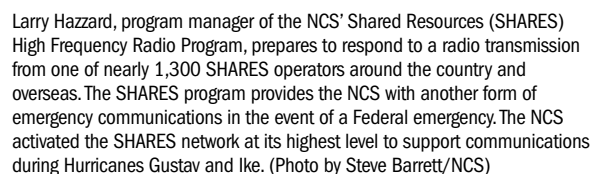
- ▶ Continued development and orchestration of cross-sector forum discussions with other ISACs for the purpose of identifying interdependencies and cross-sector vulnerabilities;
- ▶ Participated in NCC Day activities in April 2008. NCC Day was a day-and-a-half meeting with DHS, NCS, and NCC senior leadership discussing the unique industry-Government partnership and the role the COMM ISAC plays in NS/EP disaster response;
- ▶ Participated with the NCS in exercises designed to test ability of Federal Government and private industry to respond to incidents of national significance. These exercises included:
  - TOPOFF 4;
  - ESF #2 Winter Training Workshop;
  - Cyberstorm II; and
  - NLE 2-08.

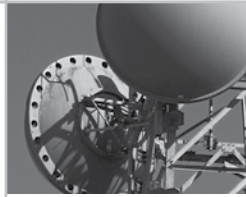
## Shared Resources High Frequency Radio Program

and critical infrastructure providers—during a disaster when normal communications are disrupted or disabled.

During FY 2008, the SHARES HF network organized and/or participated in the following training exercises and program outreach activities in addition to four SHARES activations in support of hurricanes:

- ▶ SHARES Exercise “Dark Crystal” on December 28, 2007;
- ▶ SHARES Check-In Exercise for 20-Year Anniversary on January 25, 2008; and
- ▶ SHARES Exercise “Hurricane Zoe” on May 7, 2008.





Additionally, the SHARES network conducted nearly 50 weekly exercises, three evening exercises, and participated in numerous special exercises coordinated by external entities to include:

- ▶ Cyberstorm II on March 13, 2008;
- ▶ A DOD Special Exercise on April 5-6, 2008;
- ▶ NLE 2-08 “Eagle Horizon” on May 8, 2008;
- ▶ FEMA- National Radio System (FNARS) Exercises on quarterly basis;
- ▶ Federal COOP exercises on triennial basis; and
- ▶ Quarterly SHARES “Night” checks for regions.

In addition to these exercises, the SHARES team organized and sponsored a major program milestone in recognition of 20 years of service with a SHARES open house in January 2008.

#### **Telecommunications Service Priority Program**

The FCC established the TSP Program through an FCC Report and Order on November 17, 1988. TSP provides the regulatory, administrative, and operational framework for the priority provisioning and restoration of qualified NS/EP telecommunications services. The FCC authorizes and requires service vendors to provide and restore services with TSP assignments before services without such assignments.

Currently, there are over 191,000 active TSP assignments supporting NS/EP communications nationwide. During FY 2008, the NCS added, changed, or revoked over 53,000 TSP codes. Additionally, the TSP user base increased by 114 new organizations, bringing the total number of organizations with active TSP codes to over 1,000.

In addition to daily operations, the NCS alerts TSP Program Office personnel of Presidentially declared disasters, activation of the National Response Platform, ESF #2, and COOP Plan activations. During FY 2008, the TSP Program Office assigned restoration and provisioning priorities for the following:

- ▶ FY 2008 tropical storms and hurricanes;
- ▶ Democratic and Republican National Conventions;
- ▶ Midwest tornados and floods;

- ▶ Federal Reserve Bank sites;
- ▶ United Nations General Assembly 63 (September 2008);
- ▶ President of Ukraine visit (September 2008); and
- ▶ DHS/Customs and Border Protection operations.

#### **Network Security Information Exchanges (NSIE) Activities**

In 1991, the NSC and the President’s NSTAC recommended the establishment of an industry-Government partnership to reduce the vulnerability of the Nation’s communications systems to electronic intrusion. The NCS and NSTAC formed separate government and industry NSIEs to exchange ideas on technologies and techniques for addressing and mitigating the risks to the public network and its supporting infrastructures.

In FY 2008, the NSIEs held bimonthly joint information sharing meetings and several ad hoc sessions to discuss topics of interest to members. These sessions included event correlation and monitoring, security metrics, and the NSIEs’ security priorities. During FY 2008, the NSIEs made frequent use of the US-CERT secure portal to collaborate when urgent security concerns arose.

The NSIEs also engage in international outreach activities. In FY 2008, the NSIE representatives participated in the groups’ annual trilateral NSIE meeting with the United Kingdom and Canadian NSIE organizations, hosted by Canada in Banff, Alberta. The event included trilateral information sharing between all the participants within each country’s NSIE organizations. For the first time, the annual trilateral meeting included guest representation from the Australia and New Zealand governments and communications industry. Future international NSIE meetings will include Australia and New Zealand as full participants. The United States will host the NSIE international meeting in 2009.

#### **Contingency Planning Team**

The Contingency Planning (CP) Team focuses on developing doctrine and operational plans within the CIP branch. The team also translates these plans into tools and learning aids to effectively assimilate key concepts, roles, and responsibilities to emergency communications team members.





## Contingency Planning

The team focuses on contingency communications planning and has primary responsibility for development and publication of the ESF #2 Annex to the National Response Framework (NRF), the ESF #2 Standard Operating Procedures (SOP), the NCS COOP Plan, the COOP Multi-Year Strategy and Program Management Plan (MYSMP), and numerous communications support documents.

The SOP augments the NRF's ESF #2 Communications Annex, which replaces the National Response Plan. The SOP defines the organizational structures that form when FEMA activates ESF #2 in response to an incident. It further outlines the roles and responsibilities of all ESF #2 supporting agencies under the NRF and the National Plan for Telecommunications Support in Non-Wartime Emergencies.



Aerial view taken on October 31, 2007, of homes destroyed in a Rancho Bernardo neighborhood due to the Southern California wildfires. (Photo by Andrea Booher/FEMA)

The NCS COOP plan identifies the NCS essential functions that must be performed to continue the NCS mission from an alternate location should NCS primary facilities become uninhabitable for a prolonged period of time. The plan identifies the personnel required to perform these functions and additional elements associated with relocation. The MYSMP defines the NCS roadmap for developing a viable COOP capability over the next five years. The MYSMP identifies resource and budget requirements that will enable NCS to achieve an effective, proven COOP capability and provides a schedule for completion of required actions.

## Preparedness Tools

The CP Team is responsible for the development of job aids to translate national plans (NRF/NECP) into specific tasks for Emergency Communications Team members. The team designed these tools to increase efficiency by providing information on specific positions so that any official could perform the tasks associated with that position.

In addition to these job aids, the CP Team produces standard operating procedures to provide direction, improve communication, reduce training time, and enhance work consistency. Standard operating procedures are general guidelines promulgated by the CP Team to promote a cohesive approach to responding to an incident.

## Regional Infrastructure

After Hurricane Katrina, the CIP Branch identified the requirement for a more robust regional presence. To satisfy this requirement, the branch developed a plan to staff two full-time NCS team members at each FEMA region. These team members, a Regional Communications Coordinator (RCC) and a Deputy RCC, will report to the CP Team Chief.

Since FY 2006, the NCS assigned contract personnel to FEMA Regions IV (Atlanta, Georgia), VI (Denton, Texas), and VIII (Denver, Colorado) to serve as RCCs. Those individuals remained in place through FY 2008. NCS submitted plans to replace these three contractors with permanent Federal employees as well as staff the remaining RCCs and all Deputy RCCs throughout the country.

In FY 2008, those RCCs responded to ESF #2 activations as required; attended emergency response planning conferences; participated in national, regional, and local exercises; aided national, regional, and local officials in emergency communications planning efforts; and established and strengthened relationships with Federal agencies, State, and local officials, and private industry throughout their respective regions.

In FY 2008, the Region VI and IV RCCs participated in drafting emergency communications plans for States in Regions I, II, III, IV, and VI. The focus of the DEC planning effort was on identifying and pursuing mitigation strategies for communications vulnerabilities while improving visibility of these critical issues at the FEMA Regions responsible for the states. Each RCC was an

active participant in meetings and teleconferences regarding the NECP in order to provide a field perspective to the national planning document.

Additionally, the RCCs assisted their respective FEMA regional staff in establishing and executing regional emergency communication coordination working groups (RECC-WG) as directed by Congress in U.S. House of Representatives Resolution (H.R.) 5441, *Department of Homeland Security Appropriations Act of 2007*. This legislation established the OEC as well as the RECC-WGs—which the NCS supports in order to improve awareness and visibility on regional communication interoperability issues across the Nation. RCCs also began a data collection effort to identify nationwide procedures for access, fuel provision, and security for individual states and territories. The NCS designed this effort to provide industry with quick references and accurate points of contact for re-entry procedures for restoration crews immediately following any type of incident.

### Operational Analysis Team

The Operational Analysis (OA) Team serves as the focal point for developing analytical assessments to ensure the availability of NS/EP telecommunications services despite threats to or disruptions of the infrastructure. In FY 2008, the OA Team focused on improving the quality, comprehensiveness, and timeliness of communications analytic products. Initiatives conducted during FY 2008 include activities in the following sections.

### Analysis Response Team

The increasing demand for complex, real-time analyses during emergency response operations highlighted a need for a coordinated analytic response across several entities of the NCS, Federal Government, and industry. To address that need, the OA Team established the Analysis Response Team (ART) in FY 2006. The ART brings together representatives from the OA Team, the NCC Watch, the NCS Technology and Programs Branch, DOD, the FCC, members of the communications industry, and other support elements. Each participant brings a unique set of knowledge, skills, and data that jointly contributes to a comprehensive analysis of the telecommunications infrastructure. During an emergency response event, the ART will be activated to work on-site at the NCS to meet the operational needs of the NCC Manager. During this reporting period, the ART refined a set of

standard operating procedures and conducted an orientation in the TADAC to ensure all members are well-prepared to respond to emergency events.

### Exercise Activities

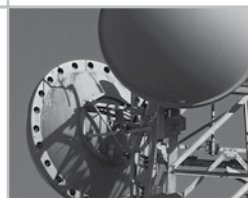
The United States faces the continuing threat of natural disasters and terrorist activity within its borders. The need for immediate response to these events increases the demand for real-time analytic capabilities during emergency response operations. The Government and its sector-specific agencies must be fully prepared to produce quality analytic products in a real-time environment in an effort to help protect and restore the Nation's critical infrastructure during the preparation, response, and recovery phases of NS/EP emergencies.

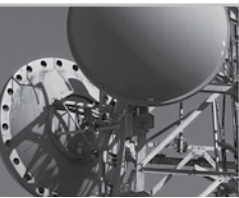
In order to ensure proper response to such events, the NCS develops government and industry exercises around specific scenarios to test and improve response and recovery capabilities. During FY 2008, the OA Team participated in the planning, conduct, and evaluation of multiple exercises to test and evaluate its analytic capabilities in response to various scenarios. The OA Team supported both pre- and post-impact scenario exercise analyses, utilized models to identify potential impacts to the communications infrastructure, represented actual impacts to the communications infrastructure, and tracked restoration activities to inform key government officials of the progress of overall restoration efforts.

During this reporting period, the OA Team provided support for the Northern Command's (NORTHCOM) Vigilant Shield 2009 exercise; DHS's TOPOFF 4, NLE 02-08, and New Madrid exercises; and the California Office of Homeland Security Golden Guardian 2008 exercise. The OA Team provided support for these exercises both on-site in the NCS TADAC and at alternate Government locations.

### Regional Characterization

In an effort to improve the ability to quickly and accurately provide critical telecommunication response assessments—especially during an emergency response operation—the OA Team initiated a series of in-depth regional telecommunications infrastructure characterizations throughout the country, and its interactions with various other infrastructures and sectors. The goal of these characterizations is to establish and document a comprehensive understanding of communication services supporting





NS/EP missions in high-risk areas prior to an emergency event. This process significantly reduces the preliminary research and data-gathering time normally associated with any analysis.

As part of these characterizations, the OA Team is coordinating with key NS/EP stakeholders to better understand their specific communication services and engineered architectures supporting their critical missions. Additionally, each regional characterization identifies and provides in-depth analysis of specific agency and communications sites of particular significance in the region. The results of these studies are incorporated into the NCS analytical tools and models used to support telecommunication assessments.

During FY 2008, the OA Team completed characterization studies in the Los Angeles and New York metropolitan areas, the National Capital Region, the New Madrid Seismic Zone, and Norfolk, Virginia. The OA Team also updated FY 2006 and FY 2007 characterizations of San Francisco, Miami, Philadelphia, Boston, Chicago, Dallas, Seattle, and Atlanta to incorporate updated findings, data, and design, and to provide the most accurate and relevant understanding of high-risk areas. In addition, the OA Team further enhanced the Philadelphia Regional Characterization with on-site visits to identified “key sites” in the Philadelphia metropolitan statistical area. The OA Team coordinated with the local GSA office to contact communications and emergency support personnel for each site and visited these individuals to validate and gain further insight into the analysis of their individual sites.

### Concentration Analysis

In FY 2008, the DHS Risk Management Division requested the NCS identify bridges and tunnels where there is a potential for a concentration of communications fiber crossings. The OA Team expanded the request to analyze concentration of the physical communications infrastructure within metropolitan areas and across the United States. The purpose of the analysis was to identify potential points of concentration within the communications infrastructure. Risks to the communications infrastructure may increase at points of concentration because damage at a concentration point has the potential to affect a large segment of the telecommunications infrastructure.

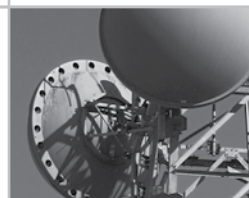
During FY 2008, the OA Team continued regional concentration studies for the major metropolitan regions within the United States, as well as a core network analysis to identify infrastructure routes that support large volumes of telecommunications traffic and locations in the long distance network where infrastructure is concentrated. The OA Team completed the analysis, documented the methodology, and incorporated the results into subsequent analyses. The NCS designed the completed effort to serve as an “on-the-shelf” product for the NCS to enhance operational understanding of the telecommunications network and augment the current understanding of the overall risks to the telecommunications sector.

### Short-Term Analysis Activities

During FY 2008, the OA Team conducted short-term analysis efforts in support of quick-turnaround information requests and emergency response operations. The OA Team employed a flexible and repeatable analysis framework with specific processes and procedures, which enabled quick-turnaround capabilities. In this quick-turnaround capacity, the OA Team collaborated with the NCC to provide analyses of the communications infrastructure and determined communications impacts due to various classes of events.



FEMA and other Federal responders work with their state counterparts in Louisiana at the mock hurricane exercise. The state emergency operations center was activated to test preparedness and response before the start of the 2007 hurricane season. (Photo by Manuel Broussard/FEMA)



During this reporting period, the OA Team provided support for events such as California's wildfire control effort, the Democratic and Republican National Conventions, the Miami power outage, the June 2008 Midwest flooding events, Hurricane Dolly, and a site-specific request from Robert D. Jameson, the DHS Under Secretary for National Protection and Programs and NCS Manager. Following each event, the OA Team investigated lessons learned to review and update processes and procedures to ensure the readiness of the OA Team in providing quick-turnaround analytical support.

### Dependency Analysis

In FY 2008, the OA Team began developing an approach for the NCS to address mega-catastrophes. The approach consists of conducting a series of analyses designed to support the NCS in its responsibilities to ensure continuity of communications for Federal agencies in the event of a major disaster. Analysis results serve to provide the NCS with a better understanding of communications infrastructure vulnerabilities, and will also assist the NCS in fulfilling its duties as prescribed by:

- ▶ NSPD 51/HSPD 20; and
- ▶ E.O. 12472.

The NCS designed this effort to perform communications dependency analyses of Federal essential functions using a predefined set of threat scenarios defined by the OA Team.

### Training and Exercise Team

The Training and Exercise (T&E) Team is responsible for ensuring a cadre of skilled civilian and military reservist personnel is ready to provide emergency response support during crises and emergencies. During FY 2008, the T&E Team successfully planned, coordinated, and performed the following activities:

#### Emergency Support Function 2 Training Conferences

The 2005 hurricane season clearly demonstrated that emergency response personnel needed the NCS' traditional ESF #2 conferences to continually address the emergency response needs of a catastrophic event the magnitude of Hurricane Katrina. Consequently, the ESF #2 T&E Team of the CIP Branch continued the training methodology of the previous year to address

the deficiencies highlighted during national and regional disasters. This resulted in the modification of the training and exercise program to improve ESF #2 staff members' proficiencies with the revised ESF #2 plans, procedures and operational support systems, as well as reinforce their roles and responsibilities as members of the ESF #2 Emergency Communications Team—ready to respond to any communications infrastructure crisis or emergency condition.

The NCS schedules ESF #2 Training Conferences twice annually, and they consist of a myriad of various training topics and exercises, which the NCS uses to educate, exercise, and provide hands-on experience for ESF #2 team members. The training conferences ensure that the ESF #2 members develop as response teams with diverse functional telecommunication skill sets enabling them to perform the ESF #2 missions.

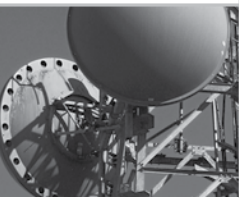
#### FY 2008 Winter Training Conference

On November 27-28, 2007, the NCS conducted an ESF #2 Winter Training Conference for over 150 attendees in McLean, Virginia. This conference focused on reviewing the lessons learned from the 2007 hurricane season and other catastrophic events during the preceding year that required deployment of ESF #2 resources and support. Additionally, the conference focused on the Emergency Communications Team's decision-making processes during disasters, and highlighted the features of the new NRF. To amplify the instruction, a presentation on team decision making ended with a series of breakout sessions involving the attendees in a sequence of decision-making exercises. The conference also featured presentations of updated organizational policies, procedures, and program resources that support the operation of the Emergency Communications Team.

#### FY 2008 Training

In January 2008, the NCS decided to temporarily suspend sponsorship of the 2008 ESF #2 Spring Conference due to program funding limitations. To continue the training momentum, ESF #2 team members need to maintain readiness; the ESF #2 Training Program evolved to incorporate traditional in-residence training and distance-learning formats. The NCS held a traditional classroom training session for DEC branch directors from May 20-21, 2008. This session discussed the roles and responsibilities of the DEC Branch Director (also known as a Federal Emergency Communications Coordinator [FECC]), which resulted in the development of the FECC Job Aid and guidelines for management of the Emergency





Communications Team. The NCS provided refresher training on the Incident Command System and team member responsibilities. The agenda also provided training on Homeland Security Information Network (HSIN), the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), and Land Mobile Radio services.

The FECC recommended providing more training for the entire team. As a result, the NCS developed a series of ESF #2 teleconference training topics and training began during July on a monthly or bi-weekly schedule to help prepare all team members for a disaster. ESF #2 team members received teleconference training sessions on deployment preparation organization of the Disaster Emergency Communications Branch, the Stafford Act, and the capabilities of the Public Safety Answering Point (PSAP) 9-1-1 facilities.

### NCS Individual Mobilization Augmentee Program

The NCS continued sponsorship of its Individual Mobilization Augmentee (IMA) program, which provides a valuable resource of skilled Army Reserve personnel to augment telecommunications response activities. This program provides the NCS with a surge capability to deploy and react to a myriad of situations associated with ESF #2 operations. Some of these Reserve officers are communications professionals in their full-time civilian careers, and are able to apply their skills when responding to Federal emergencies. The IMAs may activate and deploy to assist the NCS staff, or they may deploy to regional locations to assist during disaster response and planning.

During FY 2008, NCS IMAs continued to support the ESF #2 Team during exercises and deployments. In response to the increased frequency and duration of duty deployments, the NCS IMA Unit increased its personnel strength to the current roster of 20 officers. Officers from the IMA Unit joined the NCS Regional Managers to represent ESF #2 in the following exercises: TOPOFF 4 (Oakland, California, and Mesa, Arizona) and NLE 2-08 (Fort Lewis, Washington, and Washington, D.C.). The ESF #2 training conferences are also important training events for the IMA unit. These events provide opportunities for the military officers to train with their civilian team members, with whom they will work during emergency operations.

In addition, the officers perform individual training sessions (“battle assemblies”) to expand their knowledge and proficiency in emergency management by completing FEMA’s online training courses, attending in-residence courses at the FEMA Emergency Management Institute, and by participating in regional training events and meetings. In August, three IMA officers had the unique opportunity to join the ESF #2 team that deployed for on-site support during the Democratic National Convention. The IMA unit also provided extensive staffing support for ESF #2 operations during the 2008 storm season, deploying for Hurricanes Dolly, Gustav, and Ike, as well as Tropical Storm Hanna.

### ESF #2 Exercises

In preparation for the 2008 Hurricane Season, DHS sponsored multiple exercises to assess the capabilities of Federal, State, and local governments and private industry to respond to catastrophic events. The NCS partnered with various agencies, including GSA, FCC, NTIA, FEMA, and the U.S. Department of Agriculture, to plan and execute ESF #2 responsibilities as a major participant in the following exercises:

- ▶ TOPOFF-4 (sponsored by DHS);
- ▶ CyberStorm II (sponsored by DHS/NCSD); and
- ▶ NLE 2-08 / Eagle Horizon 2008 (sponsored by DHS).

The NCS demonstrated dedicated involvement with each of these exercises by providing realistic, coordinated communications impact analyses and scenario-based injects to support the exercise play.

### North Atlantic Treaty Organization’s (NATO)—Civil Communications Planning Committee (CCPC)



The CCPC is responsible for civil communication matters under NATO civil emergency arrangements. Civil communication planning provides for the maintenance of communication services for political, economic, and military purposes. In this context, the term “civil communications” is seen as telecommunication facilities and services, both



public and leased, postal services and any other related services provided by NATO countries, excluding military-owned and NATO-owned telecommunications facilities.

The U.S. Department of State detailee to the NCS serves as the head of the U.S. Delegation to the CCPC; the standing U.S. delegation consists of the head, U.S. Postal Service representatives, and an NCC industry representative. The U.S. delegation attends multiple CCPC working group meetings throughout the year.

### Plans And Resources Branch

The Plans and Resources Branch provides centralized management and oversight to the OMNCS for acquisition matters, financial matters, strategic and performance management planning activities, manpower allocations, and other human capital-related matters. The Plans and Resources Branch exercises authority and ensures accountability over all resources allocated to NCS programs.

The Division serves as the interface with the DHS directorates on financial and acquisition matters; DHS Planning, Programming, and Budgeting Execution System (PPBE) documentation and execution; and acquisition management. The branch conducts analyses and makes recommendations to the OMNCS on the optimal use of NCS resources to support mission requirements consistent with statutory and policy constraints.

### Planning

The Planning Team documents the OMNCS leadership's near-, mid-, and long-term strategic direction, vision, and priorities through the development of business plans, performance plans, future year homeland security planning (FYHSP) documentation, advanced acquisition plans, and budgetary expertise to strategic planning efforts.

The Planning Team, through the implementation of the strategic and performance plans, comprehensively evaluates organizational performance and effectiveness. The OMNCS develops NCS strategic and performance plans in response to the requirements of the Government Performance and Results Act (GPRA) of 1993. These plans embrace the GPRA concept of engaging in a cycle of strategic planning, performance planning, and evaluation of an organization's effectiveness.

### Financial Management

The Financial Team provides the overall fiscal direction to the OMNCS for day-to-day operations. The Financial Team develops and produces all PPBE-related documentation for the OMNCS, including documentation for program objective memoranda, budget estimates, the President's Congressional Justification budget submissions, and all related exhibits.

The Financial Team also leads in the development, coordination, and implementation of funding procedures as directed and provides guidance and assistance to all NCS agencies to ensure that their requirements are met. In addition, the team provides fund citations, ensuring the availability of funds and compliance with fiscal laws, regulations, and policies.

### Acquisition Management

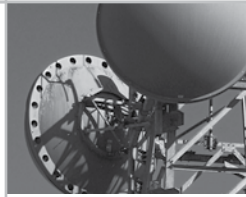
The Acquisition Team provides OMNCS divisions support throughout all aspects of the agency-level acquisition process. This includes preparing acquisition plans and strategies, statements of work, contract solicitations, proposal evaluations, and other acquisition support documentation for OMNCS programs and projects. The Acquisition Team also monitors contractual compliance, identifies contractor deficiencies, recommends contractual remedies, tracks contract expenditures, monitors all contractor reporting for accuracy, and recommends adjustments.

### Customer Service Branch

#### National Communications System Committee of Principals/Council of Representatives

President Ronald Reagan established the NCS COP in 1984 through E.O. 12472. The order outlined a broad new scope for the NCS, defining an organizational structure for the creation of a concentrated NS/EP telecommunications function, and tasked the COP with providing advice and recommendations on NS/EP telecommunications to the EOP.

The President appoints organizational members to the COP, which consists of senior-level officials representing 24 Federal departments and agencies with telecommunications facilities or services significant to NS/EP activities. The committee is a nexus for member departments and agencies to exchange ideas, coordinate interagency activity, and form recommendations on current and emerging telecommunications issues. NCS





Manual 1-2-1, *Bylaws of the National Communications System Committee of Principals*, mandates that the committee meet at least twice per year. In practice, COP meetings occur on a bi-monthly cycle and provide members with an opportunity to engage in high-level discussions regarding policy development and collaborative activities in support of NS/EP communications.

NCS Principals work in partnership on NS/EP issues, providing comments and recommendations on current and prospective national policies or programs to the NCS, the HSC, the NSC, the OMB, the OSTP, and the Executive Agent. The COP submits its recommendations directly to OMNCS; the Secretary of Homeland Security; and the President. The COP also performs any other duties or tasks the President or his authorized designee requests. Because of the increasing visibility and significance of the committee's responsibilities, Secretary of Homeland Security Michael Chertoff elevated membership of the COP to the Assistant Secretary level in FY 2007.

During FY 2008, the COP maintained an aggressive schedule of activities, including an accelerated meeting schedule, increased sponsorship of working groups, engagement in key issues, and interaction with other entities across the NS/EP spectrum. This activity included interaction with the other organizations within the DHS CS&C—the National Cyber Security Division and Office of Emergency Communications.



Kathy Blasco, a member of NCS' Critical Infrastructure Protection Branch, raises an issue of discussion during one of the many breakout sessions during the September 25-26 NSTAC Research and Development Exchange Workshop held at Motorola Headquarters in Schaumburg, Illinois. (Photo courtesy of Michael Moening/Motorola)

COP members actively engaged with the wide range of preparedness exercises taking place within the NS/EP community. Specifically, COP members participated in discussions on Cyber Storm II, NLE 02-08, and TITLE GLOBE testing. The COP also worked to establish a technical assistance team to build communications into NCS and COP member entities' exercise programs. COP member departments and agencies tracked the status of activities related to ESF #2 training. In addition, the COP spearheaded a meeting dedicated to dialogue among department and agency representatives on their organizations' preparedness plans for the 2008 hurricane season. The COP initiated discussions regarding potential changes that may be needed to NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, as well as the activities of the OEC and the National Command and Coordination Capability (NCCC).

COP members played an important role in the 2007 release of NCS Directive 3-10, providing comments to the EOP and helping to develop the capabilities of the requirements section. Moreover, COP members provided comments on the accompanying NCS Manual 3-10-1, *Guidance for Implementing NCS Directive 3-10*, and NCS Handbook 3-10-1, *Guidance for Improving Route Diversity within Local Access Networks*.

During FY 2008, the COP directed the activities of several working groups and sponsored a first-of-its-kind special event through the CDEP WG. The CDEP WG's LTO workshop brought together key personnel from the communications and electric power sectors to discuss the significance of an LTO, and begin to evaluate preparation and response strategies. The COP also voted to establish the International Communications Working Group (ICWG) to examine issues raised by the President's NSTAC Report to the President on *International Communications*. The COP, along with the NCS, continues to actively engage in responding to recommendations from the NSTAC and is currently working to develop a streamlined process to evaluate and implement appropriate recommendations in an efficient and timely manner.

### Council of Representatives

The Council of Representatives (COR) is a permanent subordinate group of the COP established by the COP Bylaws to assist in the execution of its assigned responsibilities. COR members, consisting of members of the 24 NCS departments and agencies, participate in

dedicated working groups to conduct special studies, and make recommendations to the COP on matters concerning NS/EP communications.

### Communications Dependency on Electric Power Working Group

As the governmental response to recommendations in the President's NSTAC's *Report to the President on Telecommunications and Electric Power Interdependencies*, the COP formed the CDEP WG in July 2007. The mission of the working group is to examine issues raised in the NSTAC TEPI Report, and to work in concert with the private sector to address the full set of recommendations made by the NSTAC. Additionally, the CDEP WG is working to assess a broad range of concerns inherent in the communications sector's dependence on the reliable operation of the electric power sector.

During FY 2008, the CDEP WG began the process of examining existing studies on LTOs of electric power and drafting a final report for the COP.

In an effort to gather information for its report, the CDEP WG hosted two workshops: an LTO Workshop and a Local Providers Workshop. The LTO workshop, which was the first special event hosted by the COP, included participation from 40-50 industry and Government personnel from both the communications and electric power sectors. The goals of the LTO Workshop included: raising awareness of the LTO issue and its implications; calibrating cross-sectional awareness as it applies to work flow, terminology, documents, and initiatives; obtaining input and guidance for the CDEP WG from individual experts in the communications and electric power industries; and fostering cooperation across industry sectors and between industry and Government to address the LTO issue.

The Local Providers Workshop brought together operations personnel from the major communications and electric power service providers within the Washington region. The goal of the workshop was to develop realistic communications and situational awareness strategies for use in an LTO. In addition to these activities, the working group received briefings from a number of members within the communications and electric power sectors and the Federal Government, including the Electric Power Research Institute, the Department of Energy, Bechtel, and Idaho National Laboratories.

### International Communications Working Group

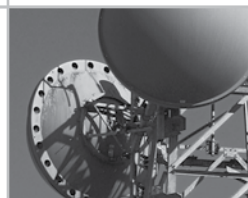
As the Government response to the President's NSTAC *Report on International Communications*, the COP voted to establish the ICWG in the Fall of 2007. Additionally, the COP charged the ICWG to work in concert with the private sector as appropriate to address the full set of NSTAC recommendations. The ICWG's charge centers on an assessment of the broad range of issues and requirements inherent in the establishment and global adoption of a framework to enhance the resilience of the global communications infrastructure.

On June 11, 2008, the COP approved the ICWG's charter, noting that initial ICWG efforts will center on an examination of existing domestic policies for international collaboration. The ICWG is currently working to prioritize its review of U.S. policy frameworks that outline the domestic process for handling global incidents. This examination will commence with a review of existing frameworks, and work toward determining how best to expand and build upon said frameworks. The group will also research existing entities to identify relevant international frameworks, policy guidance, concepts of operations, and standard operating procedures that may serve as models for the ICWG to address the NSTAC recommendations.

### Priority Services Working Group

The COP established the Priority Services Working Group (PSWG) in 2003, tasking the group with four responsibilities: (1) an evaluation of GETS, TSP, and WPS; (2) an examination of priority service outreach efforts; (3) an assessment of cost issues; and (4) an analysis of the potential impact of future technologies on priority services programs. The group's initial study examined TSP according to the four tenets of its scope of work.

In FY 2008, the PSWG updated its charter, examined next steps for studies of GETS and WPS, and made strategy recommendations aimed at improving the visibility and participation levels of priority service programs. In February 2008, the PSWG conducted an offsite visit to one of Verizon's national operations centers in Silver Spring, Maryland, to gather information on Verizon's TSP service provisioning and maintenance process and to observe a live demonstration of TSP circuit trouble-handling procedures. The PSWG also identified set procedures for business continuity planning for the TSP program databases during an emergency and gained an





understanding of Verizon's coordination and communications processes among area resources and Federal, State, and local departments and agencies. Currently, the group is writing an interim report on TSP as a direct result of some of the findings ascertained by the offsite visit to better inform the COP and the greater NS/EP community about outstanding TSP issues.

### The President's National Security Telecommunications Advisory Committee

E.O. 12382, signed by President Ronald Reagan in September 1982, established the NSTAC, as a presidentially appointed advisory committee consisting of no more than 30 industry chief executives from major communications, network service provider, information technology, finance, and aerospace companies.

In April 2008, President George W. Bush appointed Edward A. Mueller, Chairman and Chief Executive Officer of Qwest Communications as the NSTAC Chair for a one-year term. The President also designated John T. Stankey, Group President for Telecommunications Operations for AT&T, as the NSTAC Vice Chair for one year.

The NSTAC held its annual meeting on May 1, 2008, in Washington, D.C., at which time the NSTAC principals and senior Government officials reviewed the activities of the past cycle and discussed emerging issues for consideration during the NSTAC 2008-2009 Cycle. The NSTAC also met via conference call on February 28, 2008, and August 4, 2008. Discussion topics included global infrastructure resilience, the September 2008 Research and Development Exchange, the NSTAC Outreach Capstone report, traffic management, core assurance, commercial communications' reliance on GPS, network security, legislative and regulatory issues, and the NSTAC work plan.

### Industry Executive Subcommittee

During FY 2008, the NSTAC's Industry Executive Subcommittee (IES) continued to identify communications issues critical to NS/EP activities for consideration by its subgroups. The NSTAC addressed a variety of issues, including: network operations centers; NS/EP IP traffic; dependence on GPS; network security; cybersecurity policy; NSTAC outreach efforts; research and development issues; and legislative and regulatory issues. Specific subgroup activities and the results of their analysis, work, and recommendations

to the President are discussed in the following sections. The IES also received several briefings during the year to inform its activities, including:

- ▶ An overview of the FCC Vulnerability Assessment under the *Implementing the 9/11 Commission Recommendations Act of 2007 (9/11 Act)*;
- ▶ A review of the Joint Advisory Committee on Communications Capabilities of Emergency Medical and Public Health Care report;
- ▶ An update on Homeland Security Presidential Directive-8's Planning Annex;
- ▶ An overview of NSPD 51/HSPD 20;
- ▶ An overview of NCS Strategic Planning Initiatives;
- ▶ The NRF, ESF #2, and State and Local Emergency Operations Centers;
- ▶ Cyber Storm II and TOPOFF 4 Exercises;
- ▶ Priority Services for the NGN; and
- ▶ Center for Strategic and International Studies Commission on Cybersecurity.



In its 2008 report, the NSTAC Global Positioning System Working Group recommended that the President direct the DHS and DOD to include various GPS outage scenarios in future planned disaster recovery exercises. (Image courtesy of NASA)



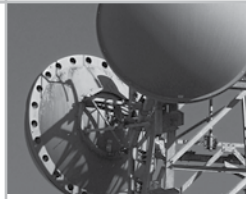
## Commercial Communications Reliance on the Global Positioning System

Throughout FY 2008, the NSTAC's Global Positioning System Working Group (GPSWG) examined information from NSTAC members, other providers within the commercial communications industry, and several external subject matter experts to evaluate the commercial communications industry's reliance on GPS, including the use of GPS in the communications, satellite, and aviation industries. As a result of this evaluation, the NSTAC developed several findings and a recommendation for consideration by the White House.

The NSTAC agreed on the following findings:

- ▶ GPS supports a broad range of commercial communications industry functions, and the primary use of GPS is in support of precise network timing and synchronization requirements.
- ▶ Another important use of GPS is support to wireless location-based services, including support of wireless Enhanced 911 (E911) Phase II requirements.
- ▶ Companies proactively employ multiple layers of backup capabilities, mitigation strategies, and contingency plans to ensure protection against a wide range of potential GPS outage or disruption scenarios. At critical nodes in the infrastructure, redundant Stratum 1-level sources are deployed and protected automatically by backup capabilities and alternate timing sources. All major carriers adhere to extremely rigorous industry-standard requirements for network timing synchronization.
- ▶ Technological, economic, and regulatory considerations necessarily factor into individual company decisions on how to mitigate the potential impact of GPS loss. While backup solutions and processes are universally implemented, specific implementations vary widely across the industry.
- ▶ Because of widely available and implemented safeguarding and mitigation strategies, short-term (less than 30 days) loss or disruption of GPS will have minimal impact on the commercial communications infrastructure and its operations. One important exception is that short-term loss or disruption of GPS signals will affect the ability to determine accurate location information for wireless E911 purposes.
- ▶ The specific consequences of medium- to long-term loss or disruption (over 30 days) of GPS will vary based on a number of factors, such as the:
  - Application being supported;
  - Duration of the disruption;
  - Geographic size of the affected region; and
  - Availability of an effective backup capability.
- ▶ The wireline network infrastructure, including wireline components of wireless, satellite, cable, and broadcast networks, will sustain operation automatically for approximately 30 days. For other components, the impact of long-term GPS loss varies.
- ▶ In the extremely unlikely event of a complete and catastrophic loss of GPS over an extended period of time (for example, more than one month) and affecting a large geographic area (for example, nationwide or global), overall impact is more difficult to ascertain. Because of the highly distributed implementations of GPS-based solutions across the industry, any impact likely would be experienced in the form of a gradual degradation of network performance, with little potential for cascading network failures. Mitigation of an extended and complete loss of GPS would require costly reconfiguration of the network to redistribute alternative timing sources. Such a reconfiguration would require a cooperative effort between carriers.
- ▶ Private sector companies have overall taken measures to safeguard against those disruptions to the GPS signal that are likely to be encountered.
- ▶ To date, no industry or Government exercise has sought to replicate the impact of a long-term or permanent GPS outage simultaneously on all industries.

At the close of its investigation in February 2008, the NSTAC recommended that the President direct the DHS and DOD to include various GPS outage scenarios in future planned disaster recovery exercises in coordination with the commercial communications industry.







## Network Operations Centers

The NSTAC reestablished the Global Infrastructure Resiliency Task Force (GIRTF) in May 2007, to address requests from DOD and the EOP. Specifically, DOD raised concerns regarding the risk to national security associated with the provisioning of network management services to domestic service providers from international network operations centers (NOC). As a result, the GIRTF reviewed relevant operations practices associated with NOCs, examined risks inherent in such operations, and outlined the steps that service providers have taken to manage those risks. In February 2008, the task force completed the NSTAC Report on Network Operations Centers, also designated For Official Use Only, to address DOD's concerns.



During the September 25-26 NSTAC Research and Development Exchange Workshop, AT&T's Rosemary Leffler (right) listens as SRI International's Zach Tudor addresses an issue in the breakout session about defending cyberspace. (Photo courtesy of Michael Moenning/Motorola)

## National Security and Emergency Preparedness NGN Traffic

In 2007, the EOP requested that the NSTAC examine the risk, if any, to IP NS/EP communications traffic during times of network congestion. Specifically, the EOP solicited NSTAC's recommendations to determine the best manner for IP NS/EP traffic to traverse the network assuming network congestion occurs. As a result, in January 2008, the GIRTF began an investigation of traffic management and priority services for IP. The NSTAC completed its Report on National Security Emergency Preparedness Next Generation Network Traffic in August 2008.

## Network Security

The NSTAC established its Network Security Scoping Group (NSSG) to research and evaluate various network security issues for possible NSTAC examination. The NSTAC recognizes that as cyber attacks and exploitation against networks increase and become more sophisticated, there is a need for both industry and Government to address the security of U.S. networks. The NSSG presented the following three issue areas to the NSTAC Principals at its May 1, 2008, Meeting:

- ▶ **Core Network Security**—The Nation's core communications networks are a collection of multiple service providers' networks that provide a high level of redundancy and service availability due to interoperation and service agreements. Congestion is a key issue for traffic moving throughout the core and may occur when network segments fail to push additional traffic onto other routes, as well as when malicious traffic floods network segments through denial of service cyber attacks. Concerns about the operation of the core network revolve around ensuring service availability, accurate delivery of content, and security of information being delivered.
- ▶ **End-to-End Network Defense**—Meeting NS/EP requirements and undertaking network defense in the NGN ecosystem, with diverse endpoints, users, applications, and networks managed by multiple entities, remains incredibly challenging. While the NGN environment enables a variety of users and devices to access the network more conveniently, it also introduces greater network vulnerability. In this diverse landscape, stronger mechanisms for ensuring trust and network management are needed to defend the end-to-end cyber ecosystem.

- **Design Issues**—The design of network equipment involves both people and processes, which increases the potential for corruption at the various development stages. Latent failure modes deal with undocumented characteristics that developers fail to discover during the functional acceptance testing stages. These modes can result from incomplete or mistaken interpretation of the specification of malicious software or hardware capabilities skillfully hidden within the gear. The key issue in this area remains the ability to assure the authenticity of the supply chain process, which is extremely difficult due to the evolving open connectivity and diversity of devices on the network.

Following the meeting, NSTAC leadership determined that the NSTAC would establish a task force to examine core network assurance issues during the course of the 2008-2009 NSTAC cycle.

### Legislative and Regulatory Issues

During FY 2008, the NSTAC's Legislative and Regulatory Task Force (LRTF) continued to closely follow laws and regulations governing NS/EP communications and related agencies and examined policy considerations of cyber warfare and cyber defense.

The task force discussed the Federal Register request for information to comply with an FCC vulnerability assessment of the Nation's critical infrastructure under Section 2201(b) of the 9/11 Act. The task force also spent time researching legislative and regulatory issues to support other NSTAC task forces, such as priority services.

The task force continued to examine the May 2007 distributed denial-of-service (DDOS) cyber attacks against the Republic of Estonia to determine whether a similar attack could occur against a U.S. Government target and its policy implications. While the attack's methods and technologies were typical of similar attacks, the attack drew the attention of the international community because it was the first time attackers had contributed to successfully disrupting a significant portion of a nation state's networks. Furthermore, Estonian officials initially speculated that the attack may have been state-sponsored, raising questions of "cyber warfare," though those assertions remain unproven. The task force anticipates completing its report throughout the 2008-2009 NSTAC cycle.

The LRTF will continue to track and analyze any resulting policies or legislation.

### Research and Development

During FY 2008, the Research and Development Task Force (RDTF) continued its efforts to examine identity management (IdM) issues. During the 2007-2008 NSTAC cycle, the RDTF focused on analyzing IdM to determine the impact on NS/EP communications. The task force developed an inventory of existing IdM-related activities occurring in industry and Government. The inventory included information on existing regulations, presidential directives, Government standards, and tools and terminology that relate to IdM. The RDTF performed a gap analysis to determine the best role for the NSTAC in IdM research and development activities is to continue to monitor and examine the development of IdM standards in the international community.



Dr. Bill Chu from the University of North Carolina-Charlotte expresses a point in discussions during a breakout session about defending cyberspace. The session was one of many topics discussed as part of the September 25-26 NSTAC Research and Development Exchange Workshop held at Motorola Headquarters in Schaumburg, Illinois. (Photo courtesy of Michael Moening/Motorola)

The RDTF also continued to track the International Telecommunication Union Telecommunication Standardization Sector's (ITU-T) IdM efforts. The task force received monthly updates on the work of the ITU-T's IdM Focus Group and Study Group 17's development of the trusted service provider identity (SPID) global standard identifier.

In March 2008, the RDTF received a briefing on European Commission (EC) activities in information and communications technology (ICT) security. During the briefing, an EC representative addressed: (1) the structure



and type of the European Union's ICT research; and (2) the need for more formalized cooperation between U.S. and European research entities.

The task force began preparations for the 2008 Research and Development Exchange Workshop, hosted by NSTAC member Motorola, Inc. at their facilities in Schaumburg, Illinois from September 25-26. The theme of the workshop was Evolving National Security and Emergency Preparedness Communications in a Global Environment. Discussion topics included IdM, emergency communications response networks, defending cyberspace, and converging and emerging technologies.

### NSTAC Outreach

The NSTAC Outreach Task Force (NOTF) operates to foster the exchange of information between key NSTAC stakeholders from both industry and Government on telecommunications-related NS/EP activities, on behalf of the Principals. The NOTF is tasked to: (1) raise the awareness of the NSTAC across industry, the Federal Government, and academic and research communities; (2) solicit feedback and input on NSTAC products and outreach initiatives from these critical stakeholders; and (3) promote the adoption of NSTAC recommendations to the aforementioned key stakeholders.

The NOTF achieved these goals during FY 2008 by:

- ▶ Finalizing a high-level NSTAC messaging document and a corresponding four-fold document, tying together the various NSTAC initiatives and successes for the purpose of stakeholder outreach;
- ▶ Submitting the NSTAC video, incorporating comments from task force and IES leadership;
- ▶ Drafting an NSTAC key terms glossary for use as a quick reference guide for NSTAC-related terms;
- ▶ Providing briefings on NSTAC reports and recommendations to key stakeholders, including meetings with several agencies in the EOP;
- ▶ Supporting the Fall 2007 IES Planning Session in Williamsburg, Virginia;
- ▶ Participating in conferences to raise the awareness of the NSTAC, including:

- The 2007 Military Communications Conference; and
- The Armed Forces Communications and Electronics Association Executive Breakfast Series;
- ▶ Drafting an NSTAC background white paper, which includes a description of key issues that the NSTAC is addressing;
- ▶ Providing an NSTAC principals orientation briefing at the 2008 NSTAC Meeting; and
- ▶ Delivering an NSTAC presentation at the 2008 Government Emergency Telecommunications Service/Wireless Priority Service Team Forum.

### NCS Issuances

As taken from NCS Directive 1-1, *NCS Issuance System*, the NCS Issuance System "governs the Issuance of rules and guidance concerning the internal organization, policies, procedures, practices, management, and/or personnel of the NCS." As necessary, the COP or its working groups may make recommendations to update existing NCS Issuances. The COP also provides comments and review for Issuances in the development process.

### Issuances or Revisions Pending during FY 2008

The issuances listed below are currently under review within the EOP, following the incorporation of edits from the NSC by the OMNCS. Following EOP review, these issuances will progress for signature to the Assistant to the President for Science and Technology and the Director of OMB:

- ▶ NCS Directive 1-1, *National Communications System Issuance System*;
- ▶ NCS Directive 1-2, *National Communications System Membership*; and
- ▶ NCS Manual 1-2-1, *National Communications System Committee of Principals By-laws*.

The following issuances are currently in development:

- ▶ NCS Handbook 3-10-1, *Guidance for Improving Route Diversity within Local Access Networks*;

- ▶ NCS Directive 3-11, *Government Emergency Telecommunications Service*;
- ▶ NCS Manual 3-11-1, *Government Emergency Telecommunications Service Manual*; and
- ▶ NCS Directive 3-12, *Wireless Priority Service*.

The following issuances were revised as recommended by the NCS COP through its PSWG Administrative Changes Report for Top-Level NCS Priority Services Guidance:

- ▶ NCS Directive 3-1, *Telecommunications Service Priority* (Currently awaiting review and edification from OSTP); and
- ▶ NCS Directive 3-3, *Shared Resources (SHARES) High Frequency Radio Program* (Returned to internal coordination process for review and coordination recommended as a result of the Hurricane Katrina After Action Report).

The following issuances were released:

- ▶ NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities* (issued by OSTP July 25, 2007); and
- ▶ NCS Manual 3-10-1, *Guidance for Implementing NCS Directive 3-10* (approved and released by NCS in February 2008).

### HSPD-7 Coordinating Councils

The communications industry established the Communications Sector Coordinating Council (CSCC) and the Federal Government established the Communications Government Coordinating Council (CGCC) in the late spring 2005 to facilitate inclusive coordination of the policy development and infrastructure-protection planning within the sector. Working together, the CSCC and CGCC finalized the CSSP in December 2006 (published in May 2007). The CSSP outlines the process for risk management in the Communications Sector, including infrastructure identification, risk assessments, protective programs, performance measurement, and research and development.

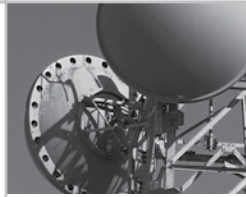
During the fiscal year, the Communications Sector focused heavily on the completion of the Communications NSRA to meet the goals of the

National Infrastructure Protection Plan and the CSSP. The NSRA identifies national-level communications architecture elements at elevated risk and serves as a baseline to prioritize the communications infrastructure. In May 2008, the CSSP Implementation Working Group, consisting of Federal Government representatives from the CGCC, industry representatives from the CSCC, and liaison representatives of the Information Technology Sector Coordinating Council, successfully completed the NSRA. The working group recommended continued discussion to identify a path forward on the following issues:

- ▶ Assessing risks associated with global communications infrastructure;
- ▶ Assessing coordinated multiple attacks;
- ▶ Assessing risks from communications dependencies;
- ▶ Assessing risks to other Critical Infrastructure Sectors, based on dependency upon communications;
- ▶ Identifying communications architecture elements at elevated risk; and
- ▶ Obtaining additional cybersecurity funding.

The Communications Sector continued to perform security-related research and development, which are vital to both the protection and the advancement of NS/EP communications as the communications sector continues its transition into NGN. The NCS, in collaboration with industry, completed a study on the impact of pandemic influenza on communications networks and continued to enhance its Internet data and NGN modeling and analysis capabilities. Over the last year, the CSCC also established the Cybersecurity Committee in response to the Government's increased attention to cybersecurity issues.

During the past year, the Communications Sector has made significant progress in completing specific actions and milestones in pursuit of advancing the seven goals detailed in its CSSP. Going forward, the CGCC and the CSCC will be working in collaboration to determine the next steps in the implementation of the CSSP. The two groups will continue to develop next-generation priority services, develop a Communications Sector outreach





program, focus on cybersecurity related programs and activities, develop sector-specific metrics, and explore follow-on activities to the NSRA.

### NCS Communications and External Affairs

The NCS—through coordination with the Department of Homeland Security's Office of Public Affairs—answers inquiries from national media outlets such as the major television networks, national wire services, leading national newspapers, Government-focused telecommunications magazines, and specialized telecommunications periodicals.

Under DHS management directives, all press releases on the NCS and NSTAC are now coordinated through both the DHS Cybersecurity and Communications external affairs director and the DHS National Protection and Programs Directorate communications director before being released by the Department. The NCS coordinates all inquiries with CS&C in conjunction with NPPD to ensure that the Department approves all requests for interviews and information about the NCS.

The 2008 hurricane season allowed the NCS to highlight its NS/EP communications role as it worked as a liaison between the NCC and ESF #15 (public affairs) to promote the NCC efforts during Hurricanes Gustav and Ike. The NCS released daily information on emergency communications activities through its DHS channels that FEMA, DHS, and the White House published to promote success stories and inform the public of its NS/EP communications role.

Additional news media and trade publications inquiries focused on NSTAC, the NCC and its Communications ISAC; WPS, GETS, and TSP programs; the SHARES High Frequency Radio Program and the NCS mission to work with industry in support of emergency communications.

In addition to fielding press inquiries, the NCS also distributed a variety of publications, reports, fact sheets, and brochures on NCS programs and the NSTAC. The NCS provides publications to the media, telecommunications companies, potential NSTAC membership applicants, and senior Government officials to provide background information on NCS programs and activities.

The NCS Program Manager for Communications continues to serve on a variety of DHS public affairs and external affairs committees. NCS is actively

involved in the DHS Internal Communications Committee (including the DHS Intranet Subcommittee), the DHS Web Content and Design Committee, and the DHS Branding Committee. In addition, the NCS participates in all meetings of the DHS National Protection and Programs Directorate and the Cybersecurity and Communications Branch dealing with external affairs activities.

### Outreach

The NCS continues to spearhead an active outreach effort to promote the NCS and its programs to a variety of commercial, Federal, State, local, and international audiences. NCS representatives attend and participate in Government and commercial technology symposia, as well as conferences on homeland security, information assurance, and critical infrastructure protection.

Aiding considerably in the outreach efforts are the six GETS/WPS Regional Outreach Coordinators and the three NCS Regional Emergency Communications Coordinators who address NS/EP communications issues at the State, regional, and local areas. The nine outreach coordinators travel throughout the year to promote NCS priority communications programs, provide guidance to local government officials on the Federal Government involvement for ESF #2 of the National Response Framework, and participate in local, regional, and national-level exercises designed to test emergency communications readiness.







## Web Sites

The NCS Web Site (<http://www.ncs.gov>) provides information on the NCS and NSTAC (<http://www.ncs.gov/nstac/nstac.html>). The site contains NCS and NSTAC history and information about NCS programs and NSTAC activities, as well as online versions of NCS and NSTAC publications.

The NCS also continues to work with DHS to show an NCS presence on the Department's own public site (<http://www.dhs.gov>), and has its own intranet section on the Department's DHS Online internal communications site (<https://dhsonline.dhs.gov/portal/jhtml/community.jhtml?index=4&community=PREP&id=25>).

## Footnotes

1. NCS Minutes from October 5, 2001 Meeting on Selected NS/EP Telecommunications Projects, October 9, 2001.





## NS/EP Telecommunications Support and Activities of Member Organizations



# Department of State (DOS)

## NS/EP Telecommunications Mission

### Secure Voice Program

The Department of State (DOS) continued its Operations and Maintenance phase of its Secure Terminal Equipment (STE) program in fiscal year (FY) 2008 and has begun the transition to the Next Generation secure Voice over Internet Protocol (VoIP) phone instrument, Viper. The Viper units are manufactured by General Dynamics and will replace the current 4891 STE units deployed by State worldwide. The program has acquired 270 Viper instruments for pilot deployments after successful laboratory testing was completed. The units have been deployed in support of special mission requirements in the Near East Asia (NEA) region with the pilot at three Embassies expected to take place in August of 2008.

The program continues to sponsor the Secure Voice Products Community of Interest Group (SVP-COI) to address the technical and other factors associated with the legacy secure voice instruments. The SVP-COI will provide the Department a secure VoIP solution that addresses all operational requirements to protect National Security information. Secure Voice in general is a constantly changing environment covering everything from interoperability issues, configuration management and key issues, and affecting all regions of the world. The most immediate issue is VoIP integration into the secure voice environment. Commercial telephone companies are accelerating the re-direction of voice services on the public network to VoIP infrastructure.

The Department also continues to evaluate newly introduced Secure Voice technology such as the portable Secure Mobile Environment- Personal Electronic Device (SME-PED) just recently certified by the National Security Agency (NSA). The SME-PED units (in addition to cellular based secure phone service) provide Personal Digital Assistant functions (including, e-mail and calendar).

### Anti-Virus Program

The Department's AntiVirus Program has detected and eradicated more than 157,177 viruses and blocked an all time record high of over 165,400,000 spam messages in FY 2008. Robust network design, perimeter and desktop anti-virus tools have resulted in a very successful program. In an effort to provide security awareness to the end users and to prevent unknowingly introduction

of malicious code, nearly 28,885 home use anti-virus software CDs have been distributed. This proactive measure controls virus incidents from emails or documents prepared by employees at home. The AntiVirus Program is currently conducting a pilot of Symantec Endpoint Protection (SEP) v.11 in coordination with the Vista Pilot being conducted by the Department's Bureau of Information Resources Management (IRM).

Currently there are approximately 390 systems actively using SEP v.11 on OpenNet. Due to end-of-life for ScanMail for Microsoft Exchange (SMEX) 3.x/6.2, the Virus Incident Response Team is piloting SMEX 8. There are 20 servers on OpenNet (the Department's controlled but unclassified information intranet) and three on ClassNet (the Department's classified information system). The AntiVirus staff is also integrating new state-of-the-art perimeter security appliances and software to replace the current legacy scanning technology. The new integrated system provides a scalable solution to meet the continuing increase in demand for Department services. This consolidated security approach in conjunction with the Secure AntiVirus Equipment Refresh will keep the Department's scanning technology up to date, while ensuring critical services are always available to the public as well as Department staff.

### Communication Security (COMSEC) Modernization

The Department is continuing its effort to modernize its national security encryption systems by using the NSA certified Inline Network Encryption (INE) devices, (KG-75s, and KG-175s). These new devices replace aging serial based encryption systems with internet protocol (IP) based systems that will provide new higher capacity, robust network designs which leverage traditional Government-owned communications, leased circuits, and the Internet infrastructure.

In addition to supporting the Department's State Messaging Archive Retrieval Toolset (SMART) and Internet Virtual Private Network programs, the INEs will provide the Department a gateway into the Department of Defense (DOD) sponsored Global Information Grid providing state of the art real time interagency secure communications of classified information. The program completed the worldwide deployment of the KG 235 software version 3.2, which is allowing the migration to the next generation INE (the KG-175D, also known as the TACLANE Micro). This encryption device supports Internet Protocol version 6 (IPv6) and also increases the



performance and reliability of the Department's classified networks. This third generation INE device will also ensure compatibility with other government agencies and enhance the Department's ability to share critical information in near real time.

The Department has also implemented the NSA-mandated Electronic Key Management System (EKMS). The Department's primary communications hub, its Beltsville Information Management Center, has been completely converted from paper based to electronic COMSEC keying material. In addition, electronic keying material has been deployed to all foreign missions in the European, NEA, East Asia and Pacific, and Western Hemisphere regions, and is being successfully utilized to encrypt their command and control data.

The EKMS program has also successfully piloted the distribution of "black" electronic keymat over the existing Department of State network infrastructure. The "black" electronic keymat program is now moving in to the full operational phase with deployments to our critical overseas locations. This program allows for rapid secure electronic keymat to often dangerous locations in near real time, ensuring critical communications are maintained while not putting a diplomatic courier in potential harm's way.

### Communication Security (Public Key Infrastructure)

The Department is currently operating a Public Key Infrastructure (PKI) at the high assurance level as outlined by the Federal PKI Policy Authority (FPKIPA). Working as partners, the Bureaus of IRM and Diplomatic Security (DS) have issued more than 35,000 "Smartcard" IDs to employees for building access and logon to the Department's Sensitive But Unclassified (SBU) system. PKI functionality has been installed on over 17,000 domestic and 19,000 overseas workstations. Projected completion for initial deployment is planned for the end of FY 2009.

The FPKIPA has cross-certified the Department's X.500 directory-based PKI and has allowed it to connect to the Federal Bridge Certificate Authority at the high assurance level. Efforts are currently underway to receive an additional cross-certification at the high assurance level for the Active Directory PKI. The Department's PKI user base of more than 33,000 has the ability to securely exchange digitally signed and/or encrypted SBU information with more than ten federal agencies, the

State of Illinois, and several non-government entities and certificate providers. The Department also uses PKI to secure its websites, update mobile code, patch applications, and provide access to a growing number of applications. It also provides support for Smartcard-based access to the Department of Justice, whose Bureau of Citizenship and Immigration Services (BCIS) has 103 sites around the country. BCIS estimates that PKI services provided by the Department of State have saved taxpayers more than \$800,000 annually. In addition, the PKI program actively supports the ePassport initiative spearheaded by the Bureau of Consular Affairs. This initiative, enabled through the Machine Readable Travel Document system, digitally signs the new ePassport so that U.S. immigration officials can verify that the passports presented to them are authentic and have not been tampered with. As of June 2008, this system has digitally signed over 27 million U.S. passports.

The Department continues its implementation of the Biometric Logical Access Development and Execution (BLADE) program. This application is coupled with the Department's PKI and allows users to logon to the unclassified system with only a scan of their finger and no password. This program improves system security by increasing accountability in system use and eliminating password sharing among users. Biometric logon is moving forward in several domestic offices and is currently in use at over thirty overseas locations. It is available for use at a total of 130 diplomatic facilities around the world. The BLADE overseas deployments in FY 2008 have been restricted due to current funding limitations but are expected to continue in FY 2009. The personal identify verification PKI authenticates and verifies all DOS employees by digitally signing all new employee identification badges.

### Secure Video and Data Collaboration

The Department has established a Video Program Office (VPO) to coordinate all unclassified and classified video conferencing services. The Secure Video and Data Collaboration (SVDC) program has been incorporated into the larger VPO charter and continues to provide secret-high videoconferencing services to DOS and to interagency gateway services.

The success of this growing program continues to prove itself through the increasing customer base, usage levels, and measurable cost savings. In FY 2008 the VPO supported an average of 200 multi-party classified and unclassified conferences a week. This is a considerable reduction of risk to personnel, incurred





by limiting the need to travel, is a particularly strong achievement of this program. The VPO is staffed 24x7, providing program management and customer support for conference scheduling, configuration, interagency coordination and technical assistance. The VPO now supports diverse interagency videoconferencing capabilities with DOD through networking partnerships with the Defense Information Systems Agency, U.S. European Command, U.S. Southern Command, and U.S. Pacific Command, as well as with other DOD area commands. Most recently, the VPO established technologies in its program that facilitate point-to-point conferencing abilities, allowing customers in multiple agencies to direct dial and expedite videoconference establishment. The success of this program continues to grow, and 210 foreign SVDC installations are currently online. The VPO continues to expand and to improve the technologies and capabilities of this program. One effort that is ongoing is the testing of telework video conferencing capabilities. The VPO is determining the Department's requirements while evaluating several possible technical solutions.

### Technical Security and Safeguards (TSS)

Responding to the new security vulnerabilities from the reality of the global information technology (IT) production, the Department employs dynamic Defensive Technical Counter-Intelligence methods to provide technical security and safeguards (TSS) for the Department's diplomatic posts and tenant agencies. These methods provide cost-effective, life-cycle risk management for technical integrity of IT equipment used inside the posts' Controlled Access Area and ensure the Department's IT security in a multi-faceted multi-cultural business environment. Coordination between the Department's Bureaus of IRM, DS, and Administration provide valuable information on new technology advancements to identify products that meet the requirements of the Foreign Affairs Community and the Intelligence Community's operational needs while ensuring that security is incorporated. Among the programs supported by the TSS initiatives are: the Department's interagency collaboration efforts, the Secure Voice Program, the Secure Video Program, COMSEC Modernization, Secure Video and Data Collaboration, and the Global Information Technology Modernization (GITM) Program.

### Domestic Radio Program

The Department's domestic radio program supports 24 Diplomatic Security Service (DSS) domestic field offices and the Washington, D.C. metropolitan area Washington Area Radio Network (WARN) system. The DSS offices are engaged in law-enforcement and protection activities and are mandated by the Diplomatic Security and Antiterrorism Act of 1986 (P.L. 99-399). The WARN system supports the Secretary of State and foreign dignitaries. The Department has recently completed an upgrade of all domestic Land Mobile Radio (LMR) systems to comply with the new National Telecommunications and Information Administration narrow-banding requirements. The Department's radio program office is currently implementing a project plan for the migration of all domestic LMR systems from Data Encryption Standard (DES) to Advance Encryption Standard (AES).

### Overseas Radio Programs

In support of the mandates in the *Diplomatic Security and Antiterrorism Act of 1986* (P.L. 99-399) and *National Security Decision Directive 38*, the Department owns and operates LMR and high frequency radio systems for Emergency and Evacuation purposes at 260 overseas United States diplomatic posts. These systems are designed to support citizen services, security, and emergency activities of the individual diplomatic missions. The Department's radio program office is also implementing plans for the migration of all overseas LMR systems from DES to AES. In addition, the Department's radio program office is implementing a life-cycle management plan for the LMR systems utilizing a new contract with Kenwood.

### Contingency Systems

In support of the Secretary of State's initiative on Transformational Diplomacy and to provide for communications in the event of catastrophic failures of the global telecommunications infrastructure, the Department has developed and is deploying two satellite based communications systems. The Remote Expeditionary Area Communications Hub is a small, portable, easily-to-use system geared towards the reporting officer operating in areas outside the local communications infrastructure, and currently offers remote Internet and voice access. The Mobile Information Programs Center, currently in development, offers all of the communications capabilities currently found in a Department communications center, including classified



and unclassified Department voice and data services, tailorable to the situation. These systems will operate anywhere in the world and have also been designed to be portable and easy to use.

### Global IT Modernization (GITM) Program

The GITM program, which was initiated on October 1, 2003, enables the Department to implement a disciplined approach, consolidating all modernization efforts for classified and unclassified local area networks (LANs) worldwide (overseas and domestic) under a centralized program for execution. This program protects the Department's substantial investment in IT infrastructure by modernizing the LAN segment of the Department's networks on a four-year life cycle. GITM completed the initial four-year life-cycle refresh in FY 2007 and the next refresh cycle began in FY 2008. GITM modernizes existing LANs using emerging technologies to keep pace with new business requirements, not just replacement of existing equipment. In FY 2008, 116 domestic and overseas LANs will have been modernized. In this way, equipment obsolescence is eliminated and the latest lines of business-driven requirements can be met. By providing reliable, secure, robust and scaleable LAN infrastructures, foreign affairs workers will have the necessary tools to enable communications, collaboration, knowledge management and the sharing of data and information in both classified and unclassified environments.

### State Messaging and Archive Retrieval Toolset (SMART)

The SMART Program is delivering a new set of communication tools to the Department of State. SMART replaces and enhances the current custom-developed cable systems that are difficult and expensive to support, and at a fairly high risk of failure. The current cable messaging and e-mail systems are being consolidated, from an end-user standpoint, into a single, easy to use system. Other tools being deployed under the SMART umbrella provide instant messaging, agency collaboration, and search tools for the archive and record management system.

This critical multi-year software integration and development project replaces old non-integrated systems by consolidating, centralizing, and modernizing messaging processes and systems in the Department. It

will benefit the Department by enabling employees to search, manage, archive, and retrieve the information and knowledge contained in the millions of diplomatic messages that are sent each year. It also implements the Department's overarching e-Diplomacy knowledge management and inter-agency information sharing and collaboration strategies. Overall, SMART greatly improves information security, integrity, and privacy through the collection and storage of robust metadata about SMART messages that includes: message type; dissemination/address; retrieval/restrictive captions; precedence—command/control; classification—sensitivity; disposition; and integrity—clearance/approval.

IRM is the system integrator for developing and managing the system in useful segments through an incremental, multi-vendor approach. The SMART Program Management Office reports directly to the Chief Information Officer (CIO), to ensure that expertise within the Bureau transitions seamlessly from SMART product development and deployment to operations and maintenance. The Department employs a SMART Steering Committee to represent the business users of the Department, review progress on a regular basis, and make recommendations to the Undersecretary for Management at the major control gates and decision points. The Steering Committee is briefed monthly, the CIO is briefed weekly, and the Office of Management and Budget is updated approximately quarterly, and prior to all milestone decisions and funding related actions.

The SMART program is making excellent progress. Segmented software analysis, design, development and testing are on schedule, and the Segment 1 pilot system was successfully deployed at three pilot posts in the first quarter of FY 2008. SMART segments 2 and 3 will be deployed to additional posts in the first and second quarter of FY 2009; and SMART will move into production and full world-wide deployment in the third quarter of FY 2009.



# Department of the Treasury (TREAS)

## NS/EP Telecommunications Mission

Fiscal Year 2008 Annual Report

The U.S. Department of the Treasury is the financial manager for the U.S. Government and a world leader in formulating and shaping economic policies and financial practices for the United States of America as a member of the world stage. The essential functions of the Treasury Department requiring national security and emergency preparedness (NS/EP) and Telecommunications Service Priority (TSP) program service are summarized as follows:

- ▶ Promote prosperous U.S. and World economics;
- ▶ Promote a stable U.S. and World economy;
- ▶ Manage the U.S. Government's finances effectively;
- ▶ Maintain, manage, and preserve the economic and financial management institutions of the United States, including all monetary, credit, and financial systems;
- ▶ Serve as one of the principal economic advisors to the President;
- ▶ Perform international economic and monetary control as it pertains to the well-being of the Nation;
- ▶ Manufacture currency, coins, and stamps; and
- ▶ Establish, monitor, and track methods of currency exchange and financial transactions.

## Telecommunications Staff Organization

The Department of the Treasury manages its telecommunications services through the Office of Chief Information Officer (OCIO). OCIO provides oversight and management of NS/EP support activities and the National Communications System (NCS) liaison. The OCIO is responsible for ensuring, through the exercise of program management authority, that Treasury Bureaus have access to a cost-effective, technologically sound telecommunications infrastructure for executing and carrying out their respective financial support missions.

In addition, the Treasury OCIO serves as a member of the Federal CIO Council and is responsible for ensuring the deployment of an enduring telecommunications capability and associated E-government application

services for maximizing cross-functional department integration between and among the Federal Departments of the U.S. Government. In this role, the Treasury OCIO guides, directs, and develops information technology (IT) management policies, standards, practices, and procedures for enabling the financial business functions of the U.S. Government.

Ongoing NS/EP Telecommunications Activities include:

## Treasury Communications System (TCS)

The Treasury Communications System (TCS), the Treasury Department's nationwide business communications networking infrastructure, continues to provide critical telecommunications services to Treasury Department Headquarters and its associated Bureaus. TCS is one of the largest secure, encrypted networks within the Federal Government today.

## TCS Computer Security Incident Response Center (CSIRC)

During fiscal year (FY) 2008, the TCS Computer Security Incident Response Center (CSIRC) Team significantly improved Treasury's security posture with several initiatives:

- ▶ Development of Secure Internet Access Guidelines (SIAG);
- ▶ Definition of revised Treasury Network (TNet) security requirements;
- ▶ Support for a Government Security Operations Center (GSOC); and
- ▶ Support for inter-agency collaboration and coordination against advanced persistent threats and ongoing participation in Department of Homeland Security (DHS) security efforts.

The TCS CSIRC's development of SIAG supports Department-wide comprehensive security architecture for Treasury's implementation of the Office of Management and Budget (OMB) Trusted Internet Connection (TIC) initiative. The SIAG serves as Treasury policy, establishing the required minimum set of security controls and logging levels required for any Treasury Internet Connection.



OMB's TIC initiative and the SIAG security requirements necessitated major revisions to the security architecture of the Treasury TNet, the forthcoming Treasury wide area data network to be deployed in FY 2009. The TCS CSIRC team worked with Bureaus and the TNet Program to define security requirements and key capabilities for a Treasury TIC, determine the core security services to be provided, and describe the "to be" TIC environment. TCS security monitoring tools required changes to accept the significantly larger data feeds from the TNet TIC.

The TCS CSIRC team is also supporting the implementation of Treasury's GSOC that will provide an overarching security organization to translate security data from all Treasury TIC's, identify problems, and act against threats on a coherent, Treasury-wide basis. As a first step toward establishing the GSOC, the TCS CSIRC team is serving as supporting security operations, collaboration, coordination, and incident reporting across Treasury. The TCS CSIRC has assumed the functions of the previously existing Treasury Computer Security Incident Response Center, adjusted its statement of work to reflect new requirements, and implemented a Web-based incident reporting portal. The consolidation was successfully completed on July 1, 2008. Efforts have been initiated to develop a Departmental Concept of Operations for an Interim GSOC and identify data definition standards that will define required security data feeds from Treasury organizations that desire to establish a TIC.

The TCS CSIRC provides Treasury's interface with the DHS U.S. Computer Emergency Response Team (US-CERT), actively participates in the GFIRST community, has well-established support for the DHS Einstein program, and continues to collaborate and coordinate on potential threats to the Departments' security posture.

### Digital Telecommunications Switching System (DTS)

During FY 2008, the Digital Telecommunications Switching System (DTS) Program continued to carry out its wide ranging responsibilities, providing secure access to Treasury's complex voice telecommunications infrastructure within local Treasury sites in the Washington, D.C. area, sites in suburban Maryland and Northern Virginia, and the physical interfaces to other telecommunications programs and services. The DTS network provided voice, data, and video services via analog, Integrated Services Digital Network (ISDN), Basic Rate Interface, and ISDN Primary Rate Interface services to the Treasury user community.

### DTS IT Security

The information transmitted and generated by DTS, and the DTS-specific information in Verizon's operations, administration, maintenance, and provisioning support systems are considered sensitive but unclassified. Treasury developed the DTS Security Program to meet all essential security requirements and technical guidance set forth in the following:

- ▶ Public Laws;
- ▶ Office of Management and Budget guidance;
- ▶ Government Accountability Office;
- ▶ National Institute of Standards and Technology Special Publications;
- ▶ Department of the Treasury Directives;
- ▶ DTS-specific policies and procedures set forth in the DTS System Security; and
- ▶ Authorization Agreement and its appendices.

The DTS network met Treasury's original requirements for the Authority to Operate in December 2003. The DTS System Security Plan (SSP) continuously defines the necessary actions for which Treasury is responsible and provides an overarching security framework and objectives. The DTS System Security Authorization Agreement and its appendices describe security measures that are currently in place, or that the DTS Program Management Office and Verizon plan to implement to ensure the confidentiality, integrity, and availability of DTS services and to fulfill contract requirements (for example, Government requirements such as FISMA, OMB A-130, and guidance from the 800 series of NIST Special Publications). Verizon's documentation complements the DTS SSP by describing how Verizon implements Treasury's DTS security framework and achieves the Department's security objectives for the enterprise voice network.

### Treasury Emergency Management Center Capability

As part of Treasury's Continuity of Operations Plan (COOP), Treasury Headquarters established emergency management centers (EMC) for responding and reacting to crises, disasters and emergencies. The local EMC is a "warm site" that has equipment in place and is tested at



least once a week. A second EMC is located within the Department of the Treasury's primary COOP location; this is a cold site. Both sites are fully integrated with the TCS network operations facilities for ensuring continuous operations of the Treasury Department in a crisis or emergency. Currently, a search is underway for a newer, larger, more capable local EMC. This new center will be improved and modernized based on changes in the Treasury Department's operating principles and practices and in the associated IT systems. The new center will accommodate changes that will enhance business management information systems. Both Treasury EMCs (local and COOP) are capable of High Frequency Radio (HF), secure voice, secure facsimile, and SIPRNet communications as well as unclassified voice, facsimile, and local area network operations. Secure video is available at the Treasury headquarters building and COOP site.

The COOP requirements for the Treasury Communications System have been fully coordinated and synchronized with the plans and programs operating under the Treasury Department's Office of Emergency Preparedness. The issuance of Government Emergency Telecommunications Services (GETS) cards continued to increase in FY08. All Successors to the Secretary of the Treasury have Wireless Priority Service (WPS) on their cellular telephones, and WPS has been made available to specific Departmental Office COOP team members as well as Treasury Bureaus. The acquisition of a new, expanded Treasury Emergency Management/Operations Center within the greater Washington, D.C. metropolitan area is expected to further strengthen Treasury's emergency preparedness posture.

Key operational functions and capabilities that will be expanded in FY 2008 and FY 2009 are:

- ▶ A larger, modernized Treasury local EMC with associated system monitoring and management tools;
- ▶ Additional contingency office space for senior Treasury leadership and their core emergency staff equipped with secure and unclassified equipment;
- ▶ Additional contingency communications capability;
  - Treasury is in the process of completing installation and implementation testing of a Treasury high frequency radio network in support of a NCS-3-10 requirements for emergency back up communications
- HF radios have been procured and installed at Treasury Headquarters, EMC and the Treasury Headquarters COOP site. HF radios are being installed at all Bureau COOP sites and selected Bureau headquarters locations
- This network will facilitate communications between Treasury headquarters and Bureau COOP sites at the secure level, as well as between the Treasury headquarters COOP site and FEMA at the TS level
- ▶ Additional GETS Cards are pre-positioned at all Treasury alternate operating facilities (AOF's) and EMC's so that cards can be transferred to Treasury staff to respond to immediate crises;
- ▶ Secure cell phones for senior staff (Secretary Successors) of the Treasury;
- ▶ WPS phones for senior staff of Treasury Bureaus;
- ▶ WPS phones for entire COOP team by end of FY 2008;
- ▶ Secure and non-secure video teleconferencing capability for the primary and alternate Treasury Headquarters COOP site;
- ▶ Full installation and monthly testing of unclassified voice, facsimile, e-mail, and secure voice, secure facsimile and secure e-mail for its primary COOP site and EMC;
- ▶ Acquisition of fixed-station satellite communications for the primary Treasury COOP site; and
- Treasury plans to equip its newer, expanded EMC with the same capability as soon as it is occupied and operational
- ▶ Full installation, testing, and use of E-Team (an unclassified event tracking system) in Treasury's EMC's and Bureau locations.
- Treasury Headquarters and Bureau emergency personnel have been trained utilizing E-Team during exercises Forward Challenge 2007 and Eagle Horizon 2008.





## Support for the Federal Public Key Infrastructure Development

The Department of Treasury continued to provide first-class technical, operational and leadership support in the development and use of an interoperable government-wide Public Key Infrastructure (PKI) to permit electronic transactions across Treasury and over the Internet in a secure and trusted environment.

Treasury's enterprise PKI system is capable of issuing digital certificates to over 150,000 Treasury employees and contractors, and to date it has had active participation by 11 of its 12 Bureaus. For this and other reasons, Treasury's PKI will be a critical component in the General Service Administration's (GSA) Personal Identity Verification (PIV) Managed Service Offering (MSO), as required by the Homeland Security Presidential Directive (HSPD) 12. Significant progress was made in FY07 to position Treasury's PKI components for integration with the HSPD-12 solution. Treasury, recognized as a leader in PKI, is working with GSA to assist other agencies with efforts to integrate solutions with the GSA MSO.

Continuing through FY 2008, Treasury continued to work with other agencies through the Federal PKI Shared Service Provider program. Treasury's involvement in this program allows the Department to reduce its ongoing operation, policy, and management costs by offering digital credential services to partnering agencies and sharing its PKI resources. This approach has proven highly successful. Treasury continues to develop a successful partnership with the National Aeronautics and Space Administration and is working with the Social Security Administration. Treasury is actively seeking future business engagements with other agencies, and will continue its efforts to do so over the next fiscal year.

Treasury is continuing its business relationship with the Federal Bridge Certification Authority that supports conducting "trusted" business with member agencies via a common PKI architecture. Additionally, Treasury accomplished policy and technical efforts to ensure that its PKI is aligned with the goals of the Federal Common Policy. This alignment is important to Treasury's role as an issuer of PIV certificates.

Treasury is expanding its current resources to meet forecasted demand and address requirements such as those brought about by the Department's involvement in the E-Authentication Federation and PIV, as described above. Treasury's critical Certification Authority (CA) hosts have undergone significant

recalibration over the past year; this effort will continue over the coming months to meet PIV integration objectives.

Also, Treasury is continuing its efforts with GSA as part of the E-Authentication Federation program, and is working actively with its trading partners in the financial community to ensure business is conducted seamlessly and securely.

## Public Safety/Law Enforcement Wireless Activities

The Department of the Treasury's Wireless Program Office (WPO) assists, coordinates, and serves as the primary technical, operational, and managerial advisor and executor for Department-wide wireless communications, specifically land mobile radios (LMR). The WPO has been successful in increasing its presence throughout the Department and across other Federal entities. For example, the WPO established the WPO Governance Board to provide Treasury Bureaus with a forum to coordinate wireless activities and discuss wireless communication needs to meet the Bureaus' public safety and law enforcement missions. The WPO continues to efficiently maintain Treasury's spectral assets, participate in the Integrated Wireless Network (IWN) Program, and assist Treasury Bureaus in upgrading their LMR equipment to meet the narrowband and advanced encryption standard (AES) mandates.

In FY 2008, the WPO assisted Treasury Bureaus in procuring equipment, including the AES upgrade software for subscriber units and encryption key loaders to secure the transmission of sensitive law enforcement related information (such as, tax payer information). Additionally, the Internal Revenue Service—Criminal Investigation (IRS-CI) upgraded communications interoperability and encryption capabilities in several field offices. IRS-CI has begun to enhance interoperable communications capabilities by programming subscriber units with federal interoperability channels identified by the Department of Justice's 25 Cities Project.

Additionally, Treasury continues to participate in the Interdepartment Radio Advisory Committee (IRAC) and other Federal committees (including, Federal Partnership for Interoperable Communications [FPIC]). Treasury's presence and participation at the IRAC ensures that Treasury's spectral assets are managed appropriately to meet the Department's spectrum needs for wireless public safety and law enforcement communications. In addition, to further increase



Treasury's spectrum efficiency, Treasury is actively continuing efforts for timely compliance with the National Telecommunications and Information Administration (NTIA) narrowband mandate, as well as participating in activities related to the Presidential Determination on Improving Spectrum Management in the 21st Century.

Treasury has increased participation within the IWN Program (a partnership including Treasury, the Department of Justice, and the Department of Homeland Security) to implement a joint law enforcement voice and data network to meet mission-critical requirements of the Federal Departments involved. This joint effort will provide cost and operational efficiencies across Treasury, as well as significantly enhance interoperable communications among law enforcement agencies. Treasury will continue to participate in this joint effort to ensure that it remains up-to-date on rapidly evolving wireless technologies and standards and to address public safety and law enforcement activities in collaboration with other Federal law enforcement agencies.

In conjunction with participation in the IWN, the WPO is also in the process of developing an implementation roadmap that describes a unified approach to continue to upgrade Treasury Bureaus' current LMR systems. Once completed, these enhancements and modernization initiatives will allow Treasury to respond, operate, and function in a crisis, emergency, or national disaster more effectively.

## Summary

FY 2008 NS/EP telecommunications activities contributed to providing a cost-effective, technologically sound telecommunications infrastructure for executing the Department of the Treasury's essential functions.

The Treasury TCS Program provided a secure, encrypted nationwide business communications infrastructure for Treasury Headquarters and its associated Bureaus.

The TCS Security Operations Center provided cybersecurity monitoring for the Treasury-wide network, successfully completed a significant architecture upgrade, deployed host- and network-based security monitoring and vulnerability management capabilities at key hosting facilities, implemented new processes to meet ever-expanding compliance requirements, and continued to forge relationships with DHS US-CERT and other federal and Defense organizations.

The TCS Security Assurance Program continued to make great strides in keeping its systems, as well as Bureau systems, compliant with certification and accreditation policies and procedures.

The DTS Program continued to provide secure access to Treasury's complex voice telecommunications infrastructure in the Washington, DC metropolitan area. Planned activities in FY 2009 include increased use of TSP to identify critical infrastructure on this program.

The Treasury Office of Emergency Preparedness saw an increase in GETS cards in FY 2008 as it supported continuity of operations requirements and made plans for a newer, larger, more capable local emergency management center.

Treasury continued supporting development of the Federal PKI infrastructure and made significant progress in positioning Treasury's PKI components for integration with the GSA's PIV MSO.

The Wireless Program Office has assisted Treasury Bureaus in upgrading their land mobile radio equipment and assisted in the procurement of equipment to secure the transmission of sensitive law enforcement related information (for example, tax payer information). In addition, the WPO represented Treasury in IRAC, FPIC, and other key groups to ensure effective management of Treasury's spectral assets.



## NS/EP Telecommunications Mission

Under the provisions of Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, Department of Defense (DOD) executes the following national security and emergency preparedness (NS/EP) telecommunications responsibilities:

- ▶ Provide, operate, and maintain the telecommunications services and facilities to support the President and the Secretary of Defense and to execute the responsibilities by E.O. 12333, *U.S. Intelligence Activities*, December 4, 1981.
- ▶ Ensure that the Director, National Security Agency, provides the technical support necessary to develop and maintain adequate plans for the security and protection of NS/EP telecommunications.
- ▶ Execute the functions listed in Sections 3(d) and 3(i) of E.O. 12472.

## Telecommunications Staff Organization

DOD includes the Office of the Secretary of Defense (OSD), the military departments and services within them, the combatant commands, and other agencies established to meet specific U.S. military requirements. The Defense Information Systems Agency (DISA) is a separate DOD agency under the direction, authority, and control of the Assistant Secretary of Defense (ASD) for Networks and Information Integration (NII)/DOD Chief Information Officer (CIO).

The principal staff positions concerned with NS/EP telecommunications in the OSD are the Under Secretary of Defense for Policy, the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD) (HD&ASA) and the ASD(NII)/DOD CIO.

## Current/Ongoing NS/EP Telecommunications Activities

### Critical Infrastructure Protection

DOD Directive 3020.40 assigns responsibilities to Department of Defense components for the identification, prioritization, and where appropriate, protection of DOD and non-DOD networked assets essential to project, support, and sustain military operations worldwide. The ASD (HD&ASA) serves as the principal senior advisor to the Secretary of Defense

on all matters related to the execution of Defense Industrial Base (DIB) Sector Specific Agency (SSA) responsibilities assigned under Homeland Security Presidential Directive-7, *Critical Infrastructure Identification, Prioritization, and Protection*.

A key accomplishment this past year in terms of breadth of participation and time committed by government and private sector DIB partners, has been the review and revision of the Goals, Objectives, Implementing Actions, and Metrics in the DIB Sector Specific Plan (SSP), meant to guide the critical infrastructure and key resource (CIKR) protection efforts throughout the sector. The DIB SSP outlines the DOD approach to executing SSA assigned responsibilities and forms an annex to the *National Infrastructure Protection Plan*. It complements other DOD critical infrastructure policy.

DOD has also continued to pursue an action to form Defense Security Information Exchanges (DSIE) patterned after the extant National Security Information Exchanges (NSIE). In 1991, the NSIEs were formed at the joint request of the National Communications Systems (NCS) and the National Security Telecommunications Advisory Committee (NSTAC). Today, these organizations have grown to become effective information sharing vehicles. The current NSIE organizations not only comprise telecommunications companies and their government counterparts, they also include 65 percent of the defense contractors and DOD agencies, such as U.S. Strategic Command, U.S. Northern Command, Joint Task Force-Global Network Operations (JTF-GNO), and the Defense Intelligence Agency.

In an effort to counter the growing threat from cyber attacks unique to defense industry, members have begun discussions concerning the formation of DSIEs. The new DSIEs would follow the same concept, that is there should be one government DSIE and one industry DSIE. The intent is for the two organizations to co-exist with each other and conduct joint meetings to share information that would benefit the protection of the CIKR of the DIB.

Most recently, DOD has partnered with the Department of Homeland Security and the private sector to form a DIB Cyber Security Working Group under the auspices of the DIB Critical Infrastructure Partnership Advisory Council (CIPAC). This Working Group operates under the National Infrastructure



Protection Plan framework to assess vulnerabilities of networks in the DIB and to share threat information and network best practices.

### Crisis Management System (CMS)

CMS is a secure, dedicated, high performance network that provides Net-Centric exchange of high-interest, time-sensitive information among the highest level of government decision makers. CMS, owned and operated by the National Security Council (NSC), extends the White House Situation Room point of presence to approximately 140 fixed and deployed locations worldwide. In addition, there are now more than 120 portable devices in the field and a “one case” next generation box about to begin production. CMS has started its engineering work to produce high-definition capabilities which are planned to begin deployment soon. Finally, CMS has expanded its presence in a variety of executive level aircraft and anticipates further requests to expand CMS’ presence in the near future. It is the President’s hands-on system of choice for day-to-day and crisis management.

CMS is comprised primarily of real-time interactive applications operating over a dedicated Internet Protocol (IP) backbone. The core CMS applications are the Secure Video Teleconferencing System, the Crisis Management Network, the Executive IP Phone System, the National Operational Intelligence Watch Officers Network, and the Big Shot Desktop Video Network. There are several NSC Network Operations Centers available 24x7 that provide control technical, security, and system monitoring services such as video and phone call manager, system maintenance, red and black HP OpenView monitoring, and an administrative conference meeting maker.

The tremendous growth in CMS services and sites is in direct response to a post-9/11 world. CMS provides a number of entry points for remote users particularly those that are not IP continuous presence subscribers, and who will “dial-in” through a variety of media into the network. The rendezvous point or “Meet Me” interface allows the gateways to interface large fixed network sites to contingency or mobile sites. The new digital gateways now being deployed are designed to respond to the growing number of contingency sites, most of whom will require dial-in capability. These gateways can support large numbers of participants in a single call. Additional participants can be placed in a virtual waiting room and invited to join conferences as required. In the not too distant future, CMS will

introduce High Definition Video Teleconferencing to key users and will dramatically expand the Executive IP Phone Network including additional interfaces to other voice networks. CMS will also offer expanded collaboration in a presentation mode.

### Net-Centric Operating Environment

ASD NII/DOD CIO, in coordination with the Joint Staff, continues Net Centric Operating Environment planning to deliver needed Global Information Grid (GIG) related products in time to support the execution of multiple programs. The objective is to synchronize programs, acquisitions, standards, architectures, and funding to ensure DOD has quality of service, network management, and information assurance within the GIG from an end-to-end standpoint in order to achieve net-centric operations.

### Global Positioning System (GPS)

DOD remains committed to ensuring a healthy and robust GPS satellite constellation. There are currently 31 operational satellites on orbit with an additional 14 satellites either awaiting launch or in production. During 2007, the control system that monitors the satellite constellation and maintains its precise time and position determination was upgraded to a modern distributed processing environment and procurement began on the next generation control capability which will enable full operation of signal capabilities on current and future GPS satellites. In May 2008, the contract was awarded for the next generation of GPS satellites (GPS III) planned for launch beginning in 2014.

During 2008, the NSTAC completed a study to gain a broad understanding of the use of and reliance on GPS timing within the commercial communications industry. The NSTAC discovered that GPS timing plays a fundamental role in supporting the commercial communications infrastructure and that industry employs a range of strategies to mitigate the impact of GPS loss or disruption. The NSTAC, however, recommended that the President direct the Department of Homeland Security and the Department of Defense to include various GPS outage scenarios in future planned disaster recovery exercises in coordination with the commercial communications industry.



## Global Broadcast Service (GBS)

The Global Broadcast Service, a high speed, satellite broadcast extension from the GIG, continues to be an important asset for globally deployed U.S. military forces. The service is very similar to commercial television broadcast system, such as DirectTV. The high-data rate broadcast links send a wide range of military information to small Receive Suites located worldwide. Year 2008 starts a transition from relay through payloads on the UHF Follow-On and commercial satellites to relay through Wideband Global SATCOM satellites. Over 700 Receive Suites are also continuing the migration toward use of IP to increase the utility and response to general and specific information requests from users

## National Leadership Command Capability Management Office (NMO)

In October 2007, the ASD(NII)/DOD CIO established the NMO to assure National and Defense leadership have persistent, adaptive, and integrated situational awareness and decision-support capabilities—anytime and anywhere. The NMO will:

- ▶ Provide “concentrated management” of Defense Leadership and Defense-supported interagency capabilities.
- ▶ Serve as a single point-of-contact within the Department for policy, long-range plans, programs, integrated mission advocacy, and management of decision-maker capabilities.

## Global Information Grid Mission Assurance (GIG-MA)

DOD has also established the GIG Mission Assurance tiger team to review the mission assurance posture of the GIG and its ability to support DOD Mission Essential Functions (MEFs) when faced with attacks by sophisticated adversaries. In conjunction with this effort, the Department has responded with the development of the Mission Assurance Decision Support System to link identified GIG infrastructure assets to key DOD Mission Essential Functions. This capability is being rapidly prototyped and operationally readied through DOD’s Joint Capabilities Technology Demonstrations program.

The GIG Mission Assurance Tiger Team produced recommendations to exercise the GIG under sophisticated cyber attack, improve GIG resiliency,

solidify GIG governance and improve intelligence to support mission assurance. These findings and recommendations were approved by the Deputy’s Advisory Working Group and fiscal year (FY) 2010-2015 resource requirement are being developed to implement the approved recommendations.

The DISA Transport Services Division of Network Services (GS22) continues to participate with OASD (NII)/DOD CIO in this important mission. There are areas of the network which have been identified that require diversity to insure a resilient network so as to avoid network outages and degraded services as highlighted by the SWA fiber cut in January 2008. DISA is developing a Program Objective Memorandum 10 funding initiative in concert with the OASD(NII)/DOD CIO to include in their submission to OSD

## Joint Task Force-Global Network Operations (JTF-GNO)

JTF-GNO leads and directs continuous Enterprise Services Management/Network Management, Information Assurance/Computer and Network Defense, throughout the GIG. JTF-GNO provides Situational Awareness (SA) of the GIG through the Network Common Operational Picture. It also provides command and control through a tiered hierarchy of NetOps Centers working together to assure Global Decision Superiority by maintaining near real-time SA, end-to-end management, and dynamic DOD network defense.

## Senior Leader C3 Systems–Airborne (SLC3S-A)

This Air Force sponsored system provides the capability for the President, Vice President, Secretary of State, Director National Intelligence, Secretary of Homeland Security, SECDEF, CJCS, and the COCOMs to perform national security and emergency response roles while airborne, world-wide. Senior Leadership and their designated staffs are provided access to live TV, secure/non-secure voice, data, and VTC capabilities to maintain situational awareness, collaborate, and reach-back to home station information sources. The system comprises infrastructure/networks on aircraft, air-to-ground SATCOM and line-of-sight systems, and teleports with dedicated high speed terrestrial connectivity to Air-to-GIG gateways (A2G2s) that extend services from home stations and other locations to the aircraft. Robust IA protections are implemented at a number of points in the system including the A2G2s. The SLC3S-A Global Network Operations Center provides oversight





to the system and acts as the central focal point for troubleshooting and resolving any issue to maintain maximum availability of services to Senior Leadership. SLC3S-A uses systems such as Boeing Broadband Service Network, INMARSAT, UHF MILSATCOM, VHF/FM, HF, NORTHSTAR, and Iridium for air to ground connectivity. SLC3S-A supports the VC-25A, E-4B, C-32A, C-40B, C-37A, C-20B/H, E-6B, C-9 and tactical platforms when fitted with DV comfort pallet (C-17, KC-10, C-141, C-130). Several immediate improvements were recently implemented: CMS provides TS/SCI Voice/and VTC to Senior Leadership while aboard VC-25A, E-4B, C-32A, & C40B. Carry-on Secure Telephone Instruments (STEs) replaced STU-IIIs. In the near-term, the Interim C3 Package is an initiative to provide critical capability to smaller aircraft that lack integrated networks in FY 2008. The Standard Communications Program provides fleet-wide standardization and modernization in the FY 2009-2013 timeframe.

### Combat Information Transport System (CITS)

CITS is an Air Force-wide program (AF component of the GIG) providing Net Centric war fighting capability upgrades and modernization to COCOMs and MAJCOMs worldwide in support of AF Network Operations (AFNetOps). In prior years CITS provided proven COTS network management and information protection tools to manage and protect the networks. Additionally, CITS provided operations sustainment through help desk, operator training, and Technical Orders. CITS has transitioned from a Base-centric to a MAJCOM-centric focus and is now moving to an integrated Network Operations and Security Center (NOSC)-centric fault, configuration, performance, and security management construct.

### Singularly Managed Infrastructure–Enterprise Level Security (SMI-ELS)

SMI-ELS is the Air Force enterprise initiative to re-engineer Air Force information, network, and computing resources to deliver reliable and verifiable information to the Warfighter as needed for critical decision-making while reducing implementation and sustainment costs to recapitalize the Air Force. SMI-ELS delivers this capability through exposure of authoritative, trusted data on demand to all users authorized and authenticated through an enterprise-wide security implementation, ensuring protection of AF information assets as well as network and computing resources. The

infrastructure required to deliver this capability is based on Service-Oriented Architecture (SOA) strategy, implementing mission capabilities as reusable services employing common infrastructure services such as security, hosting, federation, messaging, and other common services.

### Joint Staff, Military Departments, Services and the National Guard Bureau

The Military Departments (Army, Navy, Marines, and Air Force) have provided significant participation in the following areas:

- ▶ **National Military Command System (NMCS) Transformation**—NMCS Transformation is examining a changed threat environment, new national and departmental guidance and emerging technologies to develop a more capable and responsive NMCS. The Joint Staff is using the NMCS Configuration Steering Committee to manage the transition
- ▶ **Distributed Command Concept (DCC) Study Risk Likelihood Assessment**—The purpose of the DCC analysis, sponsored by the NMO is to advance national leadership command capabilities.
- ▶ **National/Defense Essential Functions (NEF/DEF) Alignment**—MEF Validation and primary mission essential functions (PMEF) Identification objective is to identify Services' MEFs and PMEFs that support DOD PMEFs and in-turn the NEFs to ensure functions can be continued through-out, or resumed rapidly after, a disruption of normal activities.
- ▶ **National Guard Bureau's Joint CONUS Communications Support Environment (JCCSE)**—enables reliable and timely flow of key information to support state and Federal military activities required for Homeland Defense (HLD)/ Civil Support (CS) missions. JCCSE is made up of three primary initiatives: 1) The Joint Command, Control, Communications & Computers (C4) Coordination Center (JCCC), 2) the Joint Incident Site Communications Capability (JISCC), and 3) the Joint Information Exchange Environment (JIEE).

JCCSE identifies the JCCC as one of the key organizational components that provides planning, coordination, and monitoring of NG Joint C4 capabilities in support of nationwide HLD/CS mission



requirements. The JCCC provides SA and builds the common operating picture (COP) from the incident site thru the National Guard Bureau to the COCOMS and mission partners.

JISCC is the equipment capability, as prescribed by the JCCSE, that is specifically tailored to support unique HLD/CS mission requirements. JISCC is a C-130 transportable, transit case-based system organized into five modules:

- ▶ **SATCOM Reach-back Communications Module**—Ku-band (Ka upgradeable) deployable satellite communications (SATCOM) terminal and backup reach-back capability.
- ▶ **Incident Site Communications Module**—20-25 handheld radios and a signal repeater to extend range for intra-team communication.
- ▶ **Interoperable Communications Module**—Audio gateway and radios that facilitate radio interoperability with first responders (e.g., police, fire), other Government agencies (e.g. FEMA), and non-Governmental agencies (e.g. Red Cross).
- ▶ **On-scene Command Post Integration Module**—Extension of the desktop to the incident scene; voice or IP telephones, computers, video teleconferencing, and multi-function printer.
- ▶ **Support Equipment Module**—Generators, power distribution, environmental control unit (ECU), tent, and transport trailer.

## US Transportation Command

USTRANSCOM has enhanced its contingency preparedness in several areas.

- ▶ **Exercise**—Conducted Hurricane Prep Table Top Exercise in May 2008 in preparation for the 2008 hurricane season in which the command updated its projected Aeromedical evacuation capability.
- ▶ **Defense Connect Online (DCO)**—Currently USTRANSCOM is undergoing a transition in collaboration tools. For some time USTC's primary collaboration tool was IWS. The command is implementing the use of DISA's sponsored tool, DCO. The use of DCO will eventually allow disparate locations to utilize the GIG to participate in such collaboration. USTRANSCOM is using both

tool sets until the customer base is better trained and more comfortable with its use.

- ▶ **Releasable domain**—USTRANSCOM has spent a great deal of effort to stand up a Secret Internet Protocol Router Network (SIPRNET) releasable domain within the command to service its imbedded coalition partners. While the customer base is currently small, it can be expanded for greater participation at a future date if need be and represents a collaboration capability under contingency circumstances if coalition coordination is required.

## National Command and Coordination Capability (NCCC)

DOD continued its support to the DHS and the NCCC effort. NCCC is the means to provide the President with the ability to respond deliberately and appropriately to any crisis. It includes responsive, reliable, survivable, and robust processes and systems to command, control, and coordinate operations among Federal, State, Tribal, Insular, and local governments, as well as private organizations, foreign governments, and international entities, as required.

## The Committee on National Security Systems (CNSS)

DOD is the Executive Agent for the CNSS, which is the policy making body for all issues concerning the security of national security systems (NSS) for the Federal Government. It promotes the security of these systems by providing a forum for policy discussions, setting national policy, and promulgating direction, operational procedure, and guidance through the CNSS issuance system.

Over the course of 2007, the CNSS established for the first time, a supply chain risk management strategy to guide efforts to counter threats posed by adversaries who seek to infiltrate the production of hardware and software upon which NSS rely. Additionally, in the identity assurance domain, the CNSS has adopted identity assurance technologies, measurably reducing the number of intrusions seen in DOD unclassified networks as a result of widespread use of Common Access Cards. Also, the CNSS has worked to create policy to ensure NSS are resilient and operate through or recover quickly from damage or successful attacks.



The CNSS priorities for 2008 include developing new national policies on risk management for; sanitizing information storage media used in NSS; incident detection response, recovery, and reporting technology; and use of federal cryptologic standards to protect NSS and National Security Information; further deploying secure portable electronic devices; and developing a government-wide vision and strategy for promoting the security and stability of the Internet as it evolves.

### National Security Presidential Directive 51/ Homeland Security Presidential Directive 20, National Continuity Policy

DOD, in coordination with the Department of Homeland Security, is tasked to provide secure, integrated Continuity of Government communication's capabilities. The document articulates a significant change from the Cold War posture and acknowledges a new view of the world in terms of no-notice, all-hazards scenarios and capabilities required to support National Essential Functions.



## NS/EP Telecommunications Mission

Led by the Attorney General, the broad mission of the Department of Justice (DOJ) is to enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior and to ensure fair and impartial administration of justice for all Americans.

DOJ is comprised of some 40 separate component organizations including:

- ▶ The U.S. Attorneys, who prosecute offenders and represent the U.S. Government in court;
- ▶ The major investigative agencies—the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration, and the Bureau of Alcohol, Tobacco, Firearms and Explosives—which deter and investigate crimes, and arrest criminal suspects;
- ▶ The U.S. Marshals Service, which protects the federal judiciary, apprehends fugitives, and detains persons in federal custody;
- ▶ The Federal Bureau of Prisons, which confines convicted offenders;
- ▶ The litigating divisions, which represent the interests of the American people and enforce federal criminal and civil law;
- ▶ Other major departmental components include the Justice Management Division, the Executive Office for Immigration Review, the U.S. Trustees, the Office of Justice Programs, the Office of Community Oriented Policing Services, the Office of the Federal Detention Trustee, the National Security Division, the National Drug Intelligence Center, the Community Relations Service, the Office of the Inspector General, the Office on Violence Against Women, and the U.S. Parole Commission.

Headquartered in Washington, D.C., the Department conducts much of its work in offices located throughout the country and overseas.

The national security and emergency preparedness (NS/EP) telecommunications mission for the DOJ is to assure the availability of telecommunications services in support of these essential law-enforcement functions.

## Current/Ongoing NS/EP Telecommunications Activities

The Department centralizes its NS/EP telecommunications services in the Office of the CIO (OCIO) under the Justice Management Division for all DOJ component agencies except the FBI which operates its own telecommunications services.

The Deputy Chief Information Officer, E-Government Services Staff operates and manages the Justice Unified Telecommunications Network (JUTNet); DOJ's consolidated data network. The Deputy Chief Information Officer, Operations Services Staff (OSS) operates and manages the Department's enterprise datacenters where secure interagency messaging is provided via the Defense Message System (SIPRNET), and the Justice Automated Message System and Joint Worldwide Intelligence Communications System.

The department is an active participant in the Government Emergency Telecommunications Service program, the Wireless Priority Service program, the Telecommunications Service Priority program, and the Shared Resources High Frequency Radio program.

DOJ continues its strong support of the National Communications System's goals and objectives through active participation in such forums as the Committee of Principles, the Council of Representatives, and the TSP Oversight Committee.

## Significant Accomplishments

- ▶ The Department materially completed its transition from several legacy data networks to JUTNet at nearly 2000 locations across the United States and its territories.
- ▶ JUTNet provides various levels of redundant and diverse connections at locations deemed to be critical.
- ▶ JUTNet provides service configurations to support emergency service restoral requirements including fly-away equipment configurations and mobile wireless connections.
- ▶ The Department initiated an enterprise voice services strategy to identify opportunities to leverage JUTNet and maturing Internet protocol telephony technologies to meet evolving NS/EP requirements



# Department of the Interior (DOI)

## NS/EP Telecommunications Mission

The Department's mission is to efficiently manage the Nation's natural resources. The Department of the Interior (DOI) and the U.S. Department of Agriculture co-manage the National Interagency Fire Center (NIFC) in Boise, Idaho. It is the Nation's primary emergency support resource for all-risk hazards management. NIFC provides emergency land mobile radio (LMR), satellite, and weather tracking systems from multiple radio caches strategically located throughout the United States to support wildland fire and national security and emergency preparedness activities under Emergency Support Function 2 (ESF #2). Operations are conducted in close cooperation with state, local, other federal, and tribal government emergency support activities.

## Current/Ongoing NS/EP Telecommunications Activities

DOI mission critical long distance voice and data communications is primarily provided by Verizon via the General Services Administration (GSA) FTS2001 contract. Selection of a successor service provider under the GSA's Networx contract will be accomplished in early fall 2008 with transition immediately following. DOI has already begun transition activities for its voice FTS2001 successor service provider.

DOI has completed consolidation of our bureau backbone data communications networks to a single Department-wide Multi Protocol Label Switched based architecture with enhanced network security functionality. The enhanced security functionality includes threat management, vulnerability management and assurance. In fiscal year (FY) 2009 we will be adding enterprise incident management and risk management capabilities according to National Institute of Standards and Technology (NIST) guidance.

DOI has also consolidated Internet service provider access from 33 points of presence to five throughout the Department and has applied for self-service provider status under the Office of Management and Budget Trusted Internet Connection program. DOI additionally has incorporated National Communications System functionality at each of its five consolidated gateways.

The transition of DOI's wideband LMR systems to the National Telecommunications and Information Administration mandated narrowband operation is a continuing high priority for the National Park Service and the Bureau of Indian Affairs. Efforts are continuing to

move these projects forward through the DOI's newly established National Radio and Spectrum Program Management Officer. DOI is in the final stages of re-competing our second multi-vendor, multi-year contract to supply Project 25 (P25) standard narrowband radios and supporting infrastructure to all Federal agencies, providing lower-cost standardized interoperable P25 radios. It is anticipated that this vehicle will be available in early quarter one, FY 2009.

DOI participates in the e-Gov SAFECOM program which promotes public safety radio system interoperability. DOI Key Officials, emergency coordinators, and telecommunications managers have Government Emergency Telecommunications Service cards for long distance emergency telephone communications and cellular phones with Wireless Priority Service. Secure Terminal Equipment secure telephones are used to support DOI national security programs and high frequency backup radio links are used to augment DOI emergency relocation site communications. Critical circuits on the DOI network and Bureau segments have received Telecommunications Service Priority designation.

## DOI Significant Accomplishments

In 2007 DOI signed separate memorandums of understanding with the states of Montana and Wyoming for interoperability partnerships in their statewide P25 compliant LMR systems. In 2008, DOI entered into a similar memorandum of understanding with the state of Nebraska. Also in 2008, DOI and National Telecommunications and Information Administration successfully certified through the Interdepartmental Radio Advisory Committee's Spectrum Planning Subcommittee the use of DOI's frequencies inside the State-wide system for Montana. This marks as a cornerstone for proportional sharing agreements between federal and state governmental communications providers.

Additionally, DOI is in process of reviewing potential partnerships in Oregon, Alaska, Idaho, and Wisconsin, and is updating its partnership agreement with South Dakota. In South Dakota, DOI has successfully added the last remaining site needed to complete the State's final coverage requirement. This site, Porcupine, is in the Pine Ridge Indian reservation and provides service to not only DOI law enforcement, but tribal law enforcement as well.





In 2008, DOI and Customs and Border Protection (CBP) have entered into an agreement to share common encryption keys for securing communications between DOI and CBP southwest border law enforcement officers. Implementation of this capability is currently underway.

DOI has established a joint DOI, Department of Homeland Security and NIST funded Telecommunications Service Center (TSC). The TSC provides a laboratory component level and holistic testing capability for determining manufacturer's radio equipment compliance with P25 standards and ability to work in support of incident command scenarios and systems. The LMR industry is very supportive of this effort with multiple vendors providing baseline user, infrastructure, dispatch and encryption equipment for testing.



### NS/EP Telecommunications Mission

The United States Department of Agriculture (USDA) national security and emergency preparedness (NS/EP) telecommunications mission is to support the Department's primary mission essential functions and support each of the National Response Framework Emergency Support Functions (ESF), especially ESF #4, firefighting.

### Current/Ongoing NS/EP Telecommunications Activities

The Forest Service maintains a significant cache of radios, and prepositions 20-25 mobile communications systems throughout the United States in 10 geographic regions in preparation for emergency response. The cache and prepositioned systems have been increasingly tapped during progressively longer fire and more active hurricane seasons. In addition, USDA contributes more than a dozen ESF #2 telecommunications specialists to the National Communications System (NCS) for national disaster response.

The USDA has a robust priority services program, which enlists the support of 85 staff representing each bureau and staff office. The Department manages an average of 1,500 Government Emergency Telecommunications Service cards, close to 300 Wireless Priority Service assignments, and over 100 Telecommunication Service Priority circuits.

USDA continues to strengthen its Continuity of Operations (COOP) Communications capabilities by routinely testing equipment and services in compliance with NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*.

### Significant Accomplishments

USDA has maintained a "green status" on progress towards the President's "Proud-to-be-Five" scorecard for COOP communications and significantly improved the communications capabilities of USDA Senior Leadership.

The Department enhanced the transmission response time for a logistics application that enables firefighters to request resources and monitor the status of existing resources.

The USDA added U.S. Coast Guard personnel as Communication Unit Leaders and Communication Technicians while battling vast California fires. The

Department's radio cache supplied radios/communications equipment to the California National Guard, Australian, New Zealanders, and Canadian fire crews, as well as numerous other fire departments from around the United States that have been dispatched to California. As a result USDA initiated an emergency procurement for an additional 300 radios.

USDA actively participated in the Communications Dependency on Electric Power Working Group, contributing twenty-five pages of draft material to the final report, leading discussions in team activities, and reporting progress to the NCS Committee of Principals.



## NS/EP Telecommunications Missions

The Department of Commerce (DOC) promotes job creation, economic growth, sustainable development, and improved living standards for all Americans by working in partnership with businesses, universities, communities, and workers to:

- ▶ Build for the future and promote U.S. competitiveness in the global marketplace by strengthening and safeguarding the Nation's economic infrastructure;
- ▶ Keep America competitive with cutting-edge science and technology and an unrivaled information base; and
- ▶ Provide effective management and stewardship of the Nation's resources and assets to ensure sustainable economic opportunities.

The DOC affects the daily lives of Americans in many ways. Examples include making it possible that weather reports are released and accessible by millions on a daily basis. Commerce facilitates technology that Americans use in the workplace, in industry, and at home every day. DOC supports the development, gathering, and transmitting of information essential to competitive business, and makes possible the diversity of companies and goods found in America's (and the world's) marketplaces. Commerce also supports environmental and economic health for the communities in which Americans live and it conducts the constitutionally mandated decennial census, which is the basis of representative democracy.

Agencies operating within the DOC include the Bureau of Industry and Security, Economic and Statistics Administration, Bureau of Census, Bureau of Economic Analysis, Economic Development Administration, International Trade Administration, Minority Business Development Agency, National Oceanic and Atmospheric Administration (NOAA), National Telecommunications and Information Administration, Patent and Trademark Office, Technology Administration, National Institute of Standards and Technology, National Technical Information Service, and the Office of the Secretary.

The Department continues to support the efforts of various cross governmental organizations including the National Communications System (NCS) Committee of Principals and the Committee of Representatives, the National Cyber Response

Coordination Group, the Critical Infrastructure Protection Policy Coordination Committee, and various Contingency of Operations Planning committees and forums.

## Current/Ongoing NS/EP Telecommunications Activities

The following current/ongoing DOC activities support national security and emergency preparedness objectives:

- ▶ The DOC manages its telecommunications through the Office of the Chief Information Officer's throughout the Operating Unit agencies, with varying telecommunications technologies services including Voice Over IP (VoIP), Private Branch Exchange, and other agency managed telecommunications services.
- ▶ The DOC is actively involved in Homeland Security initiatives and efforts to enhance preparedness with the necessary information technology equipment, software and hardware upgrades. The DOC Headquarters is located in the Herbert C. Hoover Building (HCHB) located in Washington, D.C. The Commerce Office of Security located in the Headquarters facility manages and supports the Commerce Emergency Broadcast System (EBS) that sends pre-recorded or ad hoc messages to every VoIP telephone in the HCHB. The EBS alerts users at their desks by turning on lights on the phones and playing audio messages through the phones' speakers and handset. A text message, identical to the audio message, simultaneously appears on the LCD screens of the phones to notify hearing-impaired occupants of the HCHB. This system integrates with the Public Address System, to alert users in common areas of the building such as hallways, bathrooms, the White House Visitors' Center, and the National Aquarium located in the Commerce headquarters building.
- ▶ To ensure that all households using antennas with analog TVs continue to have emergency preparedness broadcast available to them, and not be impacted by the switch to digital broadcast, the DOC has sponsored The Converter Box Coupon Program. The Converter Box Coupon Program is a direct result of the *Digital Television Transition and Public Safety Act of 2005*, which requires full-power television stations to cease analog broadcasts and switch to digital after February 17, 2009. Consumers who choose to transition to digital television using analog sets, may purchase a TV



converter box and receive a discount by using a coupon provided through DOC's Converter Box Coupon Program. The Coupon Program has been a success so far, issuing nearly 35 million coupons to approximately 18 million households. More than 14 million coupons have been redeemed for the purchase of a coupon-eligible converter box at participating retailers.

- ▶ NOAA has initiated a program that is referred to as "UrbaNet" in response to Congressional guidance to explore the utility of using local meteorological data in forecasting for urban areas. The first study was focused on the National Capital Region and involves the installation of monitoring stations within Washington, D.C. These stations collect and analyze meteorological data (including wind speed, direction and turbulence data) at frequent intervals to help define downwind areas of potential high risk. In so doing, DCNet is being used to help protect people from hazardous trace gases and particles dispersed in urban areas.
- ▶ The Department's Emergency Operation Center (EOC) uses the Plume Modeling system to track serious hazmat incidents (with accompanying toxic cloud release) in and around the metropolitan area. It is used by the EOC to develop information for senior Commerce officials to make tactical decisions on shelter-in-place or evacuation of the HCHB. The system operates using numerous NOAA sensors strategically located throughout the Washington, DC area. The Plume Modeling system provides information on plume directional feedback, times of travel to the targeted location, and the areas that would be affected in its path.
- ▶ NOAA has developed the Computer-Aided Management of Emergency Operations (CAMEO) program in response to chemical releases in the United States. CAMEO is a set of software modules designed to assist first responders and emergency planners access chemical property and response information, model potential chemical releases, display results on a map, and manage planning data. All modules work interactively to display critical information in an easy-to-understand manner. During a response to a chemical release, CAMEO can help decision makers quickly get the information they need for a safe, effective response. CAMEO is the most widely used chemical emergency response and planning tool in

the United States, and is used by industry, state and local governments, and Federal planners.

The DOC serves as a lead government agency implementing alternative communications technology with an emphasis on the Internet and electronic-commerce, and methods for protecting government networks. The DOC continues to promote the support and use of NCS services and programs, especially in light of recent hurricane disasters and post September 11, 2001, security programs.



## NS/EP Telecommunications Mission

The national security and emergency preparedness (NS/EP) mission of the Department of Health and Human Services (HHS) is to provide the necessary strategic and technical capabilities to prepare for and respond to, public health emergencies across all hazards. This includes assisting internal and external stakeholders in Public Health in obtaining sponsorship for various priority telecommunications programs, and assisting operating and staff divisions of HHS with NS/EP requirements. The Office of Preparedness and Emergency Operations is further responsible for ensuring that the Department has the systems and logistical support in place to coordinate the Department's operational response to acts of terrorism and other public health and medical threats and emergencies.

## Current/Ongoing NS/EP Telecommunications Activities

Each core operating division of HHS is focused on developing and implementing the necessary strategies to provide for:

- ▶ Communications on Public Health issues within the Federal Government;
- ▶ Communications on Public Health issues with State and local Cooperators; and
- ▶ Communications on Public Health issues with Non-Governmental Organizations.

Current emphasis continues to be enhancing disaster communications during all hazards events. Some of the areas include:

- ▶ Expanding our membership in the SHARED RESOURCES (SHARES) High Frequency (HF) Radio Program, and HF communications in general. By using HF during normal operations, our operators are better equipped to use them during a disaster. The Center for Disease Control and Prevention (CDC) has the National Public Health Radio Network using HF to provide the CDC, State, territorial, and local health departments with wireless communications capability. This back up communications system utilizes Automatic Link Establishment to maximize communications success using HF.

- ▶ Government Emergency Telecommunications Services (GETS) and Wireless Priority Service (WPS). HHS recently added WPS to all deployment wireless phone caches located throughout the United States and augmented our GETS stockpile cards as well.
- ▶ Assisting the Health care industry with critical infrastructure protection and program support (including grants) through the Hospital Preparedness program. This includes working with the Federal Communications Commission (FCC) to publicize available systems and best practices. Many additional health care facilities now have priority telecommunications programs such as the Telecommunications Service Priority (TSP) due in large part to the shared effort between HHS and the FCC.
- ▶ Enhancing Interoperability. By using the National Interoperable Field Operations Guide (NIFOG) as a baseline, and programming all Land Mobile Radios with a standard Federal Emergency Management Agency code plug HHS is more able to ensure its field teams are equipped to communicate with State and Local partners during an event. All field teams now have copies of the NIFOG in their cache.
- ▶ Increasing portable repeater cache. The Department has purchased a number of portable repeater kits, including man portable mast systems to enable our deployed teams to communicate over wider areas during an event. A number of these kits are pre-deployed in HHS response support vehicles located throughout the United States.
- ▶ Continue the implementation of applicable portions of National Communications System Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, such as Secure Satellite phones, Secure HF radio and GETS, WPS, and TSP for all personnel and circuits involved with continuity of operations.





# Department of Transportation (DOT)

## NS/EP Telecommunications Mission

The Department's mission as outlined in the Department of Transportation (DOT) Strategic Plan, asserts that the Department will "serve the United States by ensuring a safe transportation system that furthers our vital national interests and enhances the quality of life of the American people."

This core mission of the Department is constant. We remain flexible to the ever expanding global economic environment.

## Current/Ongoing NS/EP Telecommunications Activities

The Department participates in the National Communications System (NCS) Committee of Principals and Committee of Representatives, The President's National Security Telecommunications and Advisory Committee, and actively supports NCS national security and emergency preparedness activities and programs. DOT provides a member of the Chief Information Officer's staff who, as a representative, ensures that program information as provided by NCS is properly disseminated throughout the agency and the resulting benefits realized.

## Government Emergency Telecommunications Service (GETS/WPS)

The Department of Transportation continues to be involved with the Government Emergency Telecommunications System (GETS) and Wireless Priority Service. The GETS calling cards are assigned to Regional Emergency Transportation Coordinators and Representatives to be used during emergency situations. DOT is able to keep in ready contact with personnel sent to regions to offer support in emergencies. The Department continues its sponsorship of Federal, state, local government, and the private sector in entering the program. The GETS card is vital to these groups to support continuity of operations and receive priority service.

## Other Emergency Support

DOT participated in the National Level Exercise sponsored by the Federal Emergency Management Agency (FEMA). In following the direction of FEMA, DOT submitted scenarios to be used in the event directly related to its operational mission. The information gleaned from the data gathered was distributed to all interested parties and resulted in an affirmative response and approach to the continuity of government in an emergency situation.

DOT participates in internal and external Continuity of Operations (COOP) communications tests to support the National Essential Functions, and perform the Department's Primary Mission Essential Functions. This ensures that the department has a viable, functional, and interoperable communications system.

These frequent tests ensure that DOT senior leadership can communicate swiftly, securely, and efficiently with both the Executive Branch and the DOT Operating Administrations (OAs) under all circumstances.

The Department of Transportation conducts internal communications tests quarterly along with the OAs to assess the viability of their communications systems (including, secure/non-secure voice, fax, and data systems). The Department, along with many other Departments and Agencies, participates in regularly scheduled inter-agency communications tests to assess the Departments/Agencies' ability to communicate with each other using an array of communications media.

On a quarterly basis, the external communications test results from each Department and Agency are reported to the Homeland Security Council. DOT demonstrates the ability to communicate during each internal and external communications test cycle.

This year, DOT initiated a "resiliency program" to provide greater options for COOP. When activated, this program allows the Secretary and a primary successor to operate simultaneously from different continuity locations. Robust and inter-operable communications, in both unclassified and classified environments are keys to the success of the resiliency program.

## Cybersecurity

The DOT launched its new Cyber Security Management Center (CSMC) on October 1, 2007. The DOT CSMC had been in the planning stages for two years and was designed to consolidate all cybersecurity incident response activities within the Department. This has been a very successful venture for the Department and the CSMC has gained much positive recognition in the Federal cybersecurity community. The DOT has also participated in several federally sponsored exercises, the most noteworthy being Cyber Storm II. As in the first Cyber Storm exercise, the transportation sector was a primary focus of this exercise.



## NS/EP Telecommunications Mission

The U.S. Department of Energy (DOE) utilizes a number of the national security and emergency preparedness telecommunications activities in support of DOE missions to advance the National, economic, and energy security of the United States. These activities include the ability to respond to natural disasters as well as adversarial situations.

### Department of Energy Headquarters

The Department presently has 1,348 Government Emergency Telecommunications System (GETS) cards and 282 Wireless Priority Service (WPS) accounts, and continues to ensure the Telecommunications Service Priority requirements are kept up to date. During the 2008 Hurricane season, GETS and WPS were used extensively in the Gulf Coast region, following Hurricane Gustav and Hurricane Ike. Along with GETS and WPS, DOE has procured equipment to meet the in-transit requirement of National Communications Systems Directive 3-10, Minimum Requirements for Continuity Communications Capabilities.

DOE participated in exercise EAGLE HORIZON 08 (EH 08), a Federal Emergency Management Agency (FEMA)-sponsored interagency continuity exercise held from May 7-8, 2008. Exercise EH 08 was the continuity component of National Level Exercise (NLE) 2-08. NLE 2-08 was an Interim NLE conducted as a scheduled exercise within the National Exercise Program, which included a FEMA continuity component, exercise EH 08; a U.S. Northern Command defense component, exercise Ardent Sentry 2008; and the annual FEMA Hurricane Preparedness Exercise. EH 08 provided DOE the opportunity to activate its DOE Continuity of Operations (COOP) Plan, deploy Headquarters COOP personnel to the alternate site, and perform Mission Essential Functions, Essential Supporting Activities, and devolution, as a means of assessing its mission readiness.

### Oak Ridge Office (ORO)

The Wide Area Radio System (WARS) provides DOE with integrated, state-of-the-art, wireless, portable radio communications for all users on the Oak Ridge Reservation and functions as a uniform communication system. This system has the capability to link with other Federal facilities in the Oak Ridge area and to connect the ORO sites with State and local government agencies. The operation of the WARS is an

integral part of DOE's communication infrastructure during emergency situations. There are approximately 4,000 users, and more to be added soon. It provides a source of immediate communication to first responders and emergency personnel, which helps to facilitate an effective response to the community. ORO is also continuing to work with local law enforcement, emergency response, and other agencies to enhance mutual aid communications.

### Savannah River Site (SRS)

SRS is in the process of replacing the security modules at the SRS Operations Center (SRSOC). The security modules allow voice encryption over the radio channels from the SRSOC radio console. This modification will allow the move from the Data Encryption Standard to the Advanced Encryptions Standard for 600 radios. The project should be completed by fiscal year 2009.

SRS Completed the High Frequency Receiver Replacement Project as part of the National Nuclear Security Administration (NNSA)/Office of Secure Transportation (OST) Command & Control System 4.2 upgrade. All work activities were completed without incident, functional tests of new systems were performed, and the South Carolina Relay Station returned to fully operational service. The improvements support the next generation of vehicle communications being deployed throughout the NNSA/OST fleet.



# Department of Veterans Affairs (VA)

## NS/EP Telecommunications Mission

### Deployable Communications

The Department of Veterans Affairs (VA) has designed, developed, and procured a standardized set of technologies and services to support emergency preparedness and response activities as well as day to day operations. These Very Small Aperture Terminal Satellite packages provide voice, video, and data network service in a single package that can be deployed to an affected area during a disaster. To extend their effectiveness, they are also used in day to day clinic operations when not supporting emergency preparedness activities. By leveraging a standard set of tools throughout the Department, VA staff can be sent in from anywhere across the country to setup and maintain the systems so that staff in the locally affected area can take care of their families if necessary.

### Centralization of Systems

VA has made great progress towards the centralization of its information technology resources. This move to highly redundant data centers will produce a more consistent implementation of these healthcare systems and will result in a significant cost savings. The movement of systems builds upon VA's great success in the centralization of its Wide Area Networking infrastructure over the past 3 years. Additionally, the VA has augmented that infrastructure by adding Multiprotocol Label Switching and a redundant carrier to provide diversity and redundancy to its network.

### Continuity of Services

The VA Nationwide Teleconferencing System (VANTS) provides 24x7 audio and video teleconferencing services for business meetings, program planning sessions, distance learning, interviews and hearings. VANTS customers include VA employees, emergency personnel, state officials, hospitals, universities and other federal government agencies, including the Department of Defense. The video teleconferencing section of VANTS consists of two bridges capable of providing multi-point videoconferences at baud rates from 112 Kilobit per second (Kbps) up to 768 Kbps. The audio section of VANTS currently has 1,512 audio ports for voice teleconferencing.

To expedite the engineering of new radio frequency assignments, the VA uses the latest frequency management software, Spectrum XXI. The VA has

joined the National Telecommunications and Information Administration in proving the viability of a Government-wide, classified data exchange to update the Government Master File (GMF) of Radio Frequency Authorizations in real time over the public switched telephone network.

VA coordinates with Defense Information Systems Agency to provide agency customers with Enhanced Mobile Satellite Services via the Iridium low earth orbit satellite constellation. In addition to the handsets assigned to hundreds of emergency responders in the field, VA has installed multi-exchange units (MXU) at geographically dispersed locations to allow the handsets to dial directly into VA facilities via the satellite network. The MXU's also provide VA facilities access to the satellite network without having to go outside of their buildings under adverse conditions. Many of the handsets are also equipped with approved Type I communications security devices to support secure voice communications.



## NS/EP Telecommunications Mission

To serve the nation and execute the national security and emergency preparedness (NS/EP) telecommunications mission, the Department of Homeland Security (DHS) engages in critical initiatives that are improving communications capabilities across all levels of government. DHS is designing, implementing, and managing communications systems that enable secure and reliable information sharing during NS/EP activities and is also developing partnerships with Federal, State, local, and tribal governments and private entities to ensure communications are in place and operational during significant incidents.

## Current/Ongoing NS/EP Telecommunications Activities

DHS is involved in the following NS/EP-related telecommunications activities:

### DHS Wireless Services

The Wireless Services Section (WS) under the DHS Office of the Chief Information Officer (CIO) supports the NS/EP mission by providing spectrum-related services (frequency management, spectrum policy and planning), funding for special projects, department-level coordination for projects that involve multiple DHS Components, representation at DHS working groups, and, in coordination with the Office of Emergency Communications (OEC), DHS representation to intergovernmental committees, and international organizations. WS leads internal DHS initiatives to improve communications for homeland security and emergency preparedness and works to ensure that comprehensive planning and coordination of critical communications resources and equipment occur to support law enforcement and key government staff.

In fiscal year (FY) 2008, NS/EP accomplishments by WS included:

- ▶ Provided spectrum coordination and interoperable and emergency communications support to DHS Components and frontline responders during the Iowa floods and several tropical storms and hurricanes in accordance with the National Response Framework;
- ▶ Provided spectrum support for Federal Protective Service events such as the Papal visit, and the Democratic and Republican National Conventions;

- ▶ Provided detailed review and input for standard operating procedures associated with the Emergency Support Function 2–Communications (ESF #2). During emergency activations of ESF #2, WS personnel served as ESF #2 team members, supporting operations;
- ▶ Supported numerous frequency requests from U.S. Customs and Border Protection (CBP) and other agencies for use with land mobile operations and intrusion detection radar systems along the Mexican border;
- ▶ Successfully vacated the radio spectrum between 1710-1755MHz auctioned to commercial carriers for Advanced Wireless Services (AWS) within the one-year timeline in accordance with the program and the procedures prescribed by the Office of Management and Budget, the Federal Communications Commission, and the National Telecommunications and Information Administration (NTIA);
- ▶ In cooperation with the OEC, WS continued to support the National Interoperability Frequency Guide and the National Interoperability Field Operations Guide;
- ▶ Coordinated with NTIA to establish a consolidated joint government-industry interference testing program;
- ▶ DHS CIO funded CBP and U.S. Immigration and Customs Enforcement Operations and Maintenance for radio systems. Additionally, WS funded the NTIA Spectrum fees for the Department; and
- ▶ DHS continues to support the Components by performing the five-year NTIA Spectrum reviews.

### Homeland Secure Data Network

As of the end of FY 2008, the DHS deployment of the Homeland Secure Data Network (HSDN) reached 112 government sites, providing a unified system and program that enables the sharing of secret-level data between its Federal partners. The HSDN continues to significantly enhance DHS' capability to interact with other classified networks while simultaneously eliminating the Department's dependence on networks external to DHS. HSDN is the single program within DHS that enables agencies to collaborate and communicate effectively at a SECRET-classified level among Federal and



State government and supporting entities. With HSDN capabilities, DHS has the ability to collect, disseminate and exchange both tactical and strategic intelligence information throughout DHS and DHS partners.

In fiscal year (FY) 2008, HSDN accomplishments included:

- ▶ Established and maintained periodic HSDN program self-assessment and evaluation through the DHS established Operational Analysis periodic review and reporting process, for identifying areas for improvements in costs and operational efficiencies and effectiveness;
- ▶ Established support to the mission requirements of DHS component organizations and its homeland security partners staying abreast of and identifying applicable advancing information and applied technologies capable of improving data gathering, fusion, analysis, intelligence gathering and dissemination at a SECRET-classified level;
- ▶ Supported the National Command and Coordination capability Funding (NCCC) effort as a key member of the NCCC working group, developed NCCC overall architecture and GFE re-use, and developed a pilot plan for Secure Mobile Environment Portable Electronic Device (SME-PED) and deployed a SME-PED test environment;
- ▶ Identified a closed storage solution, developed by DTECH Labs, that fits in a standard Mosler safe drawer, collaborated with L3 to address and correct talon short-comings (failover, multiple sign-ons, and lack of Firefly keys), coupled solution with a Thin Client laptop capability. Completed the integration of the DTECH closed storage solution and successfully deployed the first five units;
- ▶ Completed the integration of the L3 Talon to provide a low cost HSDN solution (successfully deployed the Talon solution to Department of Transportation Crisis Management Center). The Talon is a NSA certified encryptor that enables users to securely access network resources at levels up to TS/SCI from virtually any location;
- ▶ Successfully deployed 31 new sites (including four Other Government Agency sites—Nuclear Regulatory Commission (three sites) and Department of Energy (one site)) and includes two HSDN sites to support the Democratic and Republican National Conventions;
- ▶ Successfully implemented a solution to provide connectivity for the Transportation Security Administration Trace system to HSDN (provides SIPRNet connectivity and provides Trace users HSDN email);
- ▶ Completed the Info Work Space Pilot implementation for the I&A;
- ▶ Successfully transitioned the I&A web hosting application into the HSDN Demilitarized Zone infrastructure;
- ▶ Completed the transition from the Coast Guard High Assurance Guard (HAG) to the Defense Information Systems Agency HAG; and
- ▶ Supported the National Continuity of Operations Planning exercise in May.

### Office of Emergency Communications

The DHS OEC was established by Public Law 109-295, the Post-Katrina Emergency Management Reform Act of 2006. Director Chris Essid leads OEC to support and promote the ability of emergency responders and government officials to communicate in the event of natural disasters, acts of terrorism, or other man-made disasters, and work to ensure, accelerate, and attain interoperable and operable emergency communications nationwide.

OEC absorbed some of the functions of the former ICTAP, Wireless Management Office, SAFECOM, and the Federal Partnership for Interoperable Communications. Since commencing operations on April 2, 2007, OEC's accomplishments include:

- ▶ Developed the National Emergency Communications Plan in coordination with over 150 Federal, State, and local emergency response practitioners;
- ▶ Coordinated the development, review, and approval of all 56 Statewide Communication Interoperability Plans for DHS





- ▶ Developed grant guidance for the FY 2008 Interoperable Emergency Communications Grant Program, in coordination with the Federal Emergency Management Agency, which awarded \$48.5M to all 56 States and territories; and
- ▶ Developed the Type III Communications Unit Leader (COML) training curriculum, in coordination with the Office for Interoperability and Compatibility. OEC now administers the training, resulting in over 240 COML certifications by the end of October 2008.



# Office of the Director of National Intelligence (ODNI)

## NS/EP Telecommunications Mission

The national security and emergency preparedness telecommunications mission of the Office of the Director of National Intelligence (ODNI) is to ensure the secure flow of all-source foreign intelligence information to the President, and other selected national policy makers. To this end, ODNI ensures that Intelligence Community organizations together provide secure, rapid, and reliable round-the-clock telecommunications and information services that are:

- ▶ Modern, efficient, and interoperable to support intelligence collection and distribution requirements;
- ▶ High-volume and timely for open-source collection; and
- ▶ World-wide quick reaction in support of crisis and special operational requirements.

## Telecommunications Staff Organization

Within the ODNI, the Associate Director of National Intelligence and Chief Information Officer (CIO) in their role as the Intelligence Community Chief Information Officer (IC CIO) manages activities relating to information technology (IT) infrastructure and enterprise architecture requirements of the Intelligence Community (IC), including, messaging, telecommunications, and information services capabilities.

## Current/Ongoing NS/EP Telecommunications Activities

Active participation in the National Communications System (NCS) activities of the Committee of Principals, Council of Representatives, and underlying working groups.

Active participation as a member of the Joint Telecommunications Resources Board (JTRB).

Continuing to work with ODNI Continuity Programs to assure proliferate Government Emergency Telecommunications Services, the Wireless Priority Service, the Telecommunications Service Priority, and other NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, requirements in accordance with the ODNI's Implementation plan for achieving compliance with NCS 3-10.

Continued to add redundancy and eliminate single points of failure in our commercial and secure voice and data networks.

## ODNI Significant Accomplishments

- ▶ Initial implementation of the Intelligence Community Login capability, providing the architecture for personnel from Intelligence Community agencies to access their home organization's IT infrastructure from remote locations.
- ▶ Assisted numerous departments and agencies with developing plans for compliance with the requirements for Top Secret/ Sensitive Compartmented Information connectivity now required by NCS Directive 3-10.
- ▶ IC CIO appointed by the Director, Office of Science and Technology Policy to be a member of the JTRB.
- ▶ Formally established the Mission Assurance Technology Committee, an IC-wide forum to facilitate agency awareness and implement standardized disaster recovery requirements for the IC IT/Comms infrastructure and architecture.



## NS/EP Telecommunications Mission

The mission of the Federal Emergency Management Agency (FEMA) is to reduce the loss of life and property and protect the nation's critical infrastructure from man-made and natural hazards through a comprehensive program of mitigation, planning, response and recovery. FEMA helps the nation address communications network disruptions. FEMA's main mission is to manage federal response and recovery efforts following any national incident and to serve as the nation's portal for emergency management information. FEMA evaluates and adopts new telecommunications technologies annually, to ensure that government agencies can accomplish their missions effectively, even in the event of a catastrophic commercial telecommunications Infrastructure Loss.

## Current/Ongoing NS/EP Telecommunications Activities

FEMA provides critical infrastructure support to communities, county's and States affected by natural or man-made disasters, before, during, and after destructive incidents to minimize the loss of life, assist in clean-up and recovery, and help victims return to normal activities. FEMA helps communities plan for and face the threat of terrorism, weapons of mass destruction, and natural incidents preparing communities to respond to all types of hazards. FEMA also establishes working relationships with state and local first responder and public safety communications organizations. In addition, FEMA:

- ▶ Plans for, provides, operates and maintains information technology (IT) systems, telecommunications services and facilities as part of the National Emergency Management Information System (NEMIS);
- ▶ Designs and develops emergency networks and information systems;
- ▶ Works with the commercial telecommunications industry to provide quick recovery from telecommunications infrastructure failures or outages through the Telecommunications Service Priority process;
- ▶ Provides communications support to State and local officials to help disseminate warnings of risks and hazards to the general public;

- ▶ Accumulates and assesses damage information after an incident has occurred;
- ▶ Deploys emergency telecommunications and IT network assets to incident areas to provide incident command and control during the initial hours of a disaster, and coordinates with State and Local responders to place assets where needed; and
- ▶ Coordinates the assignment and use of all Federal radio frequencies at an incident site to include high frequency (HF), ultra high frequency, very high frequency, 700 Megahertz (MHz) and 800 MHz radio frequencies. This coordination reduces area interference, crosstalk and jammed networks, creates bandwidth for outside agency utilization, and promotes interoperability among response groups.

## Significant Achievements

A Common Alerting Protocol was developed for use by public television, cellular phones, pagers, and satellites to improve the existing public Emergency Alerting System.

NEMIS supported 102 disaster and emergency declarations in fiscal year (FY) 2007. NEMIS added the EMC FAN to significantly increase data storage capability. Finally, FEMA consolidated four NPSC's into two NPSC's to improve NEMIS operations and reduce replication of data.

The Mobile Disaster Response Center program was moved under the command and control of the Disaster Response Team. This move will improve coordination for deployment and implementation of these systems throughout a disaster area. These self contained communications vehicles are used to insert command, control, communications, and interoperability into an incident area without interconnectivity to other disaster management assets. The Disaster Response Team also assumes responsibility for operations and maintenance of these systems insuring that the latest equipment, software and operating systems are available for use.

Mobile Emergency Response Support (MERS) enhancements included the establishment of interoperability requirements with other Federal, State and Local entities. This communications coordination was executed through four major communications exercises. MERS also validated the air-lift capability of the Incident Response Vehicle in 3 of the 6 MERS detachments.



The FEMA National Radio System (FNARS) multiphase upgrade project continued in FY 2007. Additional (Gulf Region) State Emergency Operating Center's were upgraded with new HF radio systems. Additional funding was secured to continue the project in FY 2007-2008. Finally, operational control of the FNARS upgrade was transferred to ONCP to put the entire program under one office.



## NS/EP Telecommunications Mission

The national security and emergency preparedness (NS/EP) telecommunications mission of the Central Intelligence Agency (CIA) is to ensure the secure flow of all-source foreign intelligence information to the Director of National Intelligence, President, and other selected national policy makers. To this end, the CIA provides secure, rapid, and reliable round-the-clock telecommunications and information services that are:

- ▶ Modern, efficient, and interoperable to support intelligence collection and distribution requirements.
- ▶ High-volume and timely for open-source collection.
- ▶ World-wide quick reaction in support of crisis and special operational requirements.

## Telecommunications Staff Organization

The Global Communications Service (GCS) operates, manages, and maintains the CIA's messaging, telecommunications, and information services capabilities.

GCS also provides telecommunications support to other U.S. Government departments, agencies, and the military services as required to support intelligence requirements.

## Current/Ongoing Telecommunications Activities

- ▶ Active participation in the National Communications System activities of the Committee of Principles/Council of Representatives.
- ▶ Continued support of the Government Emergency Telecommunications Services, the Wireless Priority Service, and the Telecommunications Service Priority system.
- ▶ Continue to transition our legacy secure telephone units (STU-III) to the new Secure Terminal Equipment.
- ▶ Continue to expand secure video teleconferencing to our workforce desktops.
- ▶ Continue efforts to be fully compliant with NCS Directive 3-10, Minimum Requirements for Continuity Capabilities.

## CIA Significant Accomplishments

- ▶ Continued to develop a cadre of professional personnel prepared to meet operation, technical, and system management requirements of state-of-the-art telecommunications and automated information systems.
- ▶ Provided enhanced telecommunications services between the CIA, other U.S. Government organizations, and the U.S. military services.
- ▶ Continued support to Defense Message System objectives and architecture.
- ▶ Continued to add redundancy and eliminate single points of failure in our commercial and secure voice and data networks.





# General Services Administration (GSA)

## NS/EP Telecommunications Mission

The General Services Administration (GSA) mission is to help Federal agencies better serve the public by offering, at best value, superior workplaces, expert solutions, acquisition services and management policies.

GSA is comprised of two integral components—The Public Building Service (PBS) and the Federal Acquisition Service (FAS). Within the FAS, the Integrated Technology Services (ITS) organization provides a broad spectrum of telecommunications and network services to the Federal departments and Agencies. The mission of the FAS-ITS is to deliver best value and innovative acquisition solutions for Information Technology (IT), Network Services (telecommunications), and Professional Services to support Government agency requirements worldwide. FAS-ITS works with agency customers to understand their requirements, simplify the development of acquisition strategies, conduct the acquisition, provide assistance throughout implementation, and manage the associated funding. FAS-ITS services help agencies achieve best value solutions and avoid doing costly, time-consuming acquisitions, save taxpayer dollars, and enable them to devote more of their own staffs directly to their agency missions and programs.

The GSA mission support functions for national security and emergency preparedness (NS/EP) are detailed in following authoritative documents:

- ▶ Executive Order (E.O.)12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*
- ▶ E.O. 12656, *Assignment of Emergency Preparedness Responsibilities*
- ▶ Office of Science and Technology Policy: *National Plan for Telecommunications Support in Non-Wartime Emergencies*
- ▶ Communications Act of 1934 (as amended), Section 706, War Emergency Powers
- ▶ National Response Plan

## Current/Ongoing NS/EP Telecommunications Activities

FAS-ITS continues to help its client agencies develop solutions using a variety of IT and Network Services contracts. FAS-ITS assists with defining requirements,

reviewing alternatives, developing performance based statements of objectives/statements of work, awarding tasks, project management, and managing project funds

FAS-ITS provides a variety of network services, information technology, and professional services that presently support 135 Federal agencies around the world. GSA's newly awarded, and highly anticipated Network Universal and Network Enterprise contracts are now available to provide voice and data services over terrestrial, wireless, and satellite transports supporting both classified and unclassified applications with integrated security features. Augmented by the availability of recently awarded SatCom-II contract, GSA Schedule 70 acquisitions, GSA Government-wide Acquisition Contracts and other integrated technology resources, GSA's Integrated Technology Services division is a one-stop shopping facility for virtually any IT requirement.

FAS-ITS provides emergency telecommunications support under the authority of the National Response Plan as detailed in the Office of Science and Technology Policy's "National Plan for Telecommunications Support in Non-Wartime Emergencies."

A Telecommunications Specialist is appointed by GSA in each Region to serve as National Communications System (NCS) Regional Manager (NCSRM). The NCS is the lead agency for Emergency Support Function 2-Communications (ESF #2). The NCSRM represents the NCS ESF #2 responsibility and efforts for regional emergency disaster response planning, training, and exercise activities. Additionally, the NCSRM builds working relationships with the telecommunications industry within their respective Federal region. This ensures a seamlessly coordinated government/telecommunications industry emergency response effort. During the pre-deployment phase, the NCSRM coordinates and assesses potential emergency telecommunications requirements throughout their assigned region. Upon activation of ESF #2 by the Federal Emergency Management Agency (FEMA), the NCSRM may transition to the role of Federal Emergency Communications Coordinator (FECC), reporting to the NCS and the FEMA Federal Coordinating Officer (FCO). During disaster response efforts, the FECC is the single Federal point of contact in the incident area to coordinate ESF #2 response and recovery with the FCO and Principal Federal Official, as necessary.



## GSA/FAS Significant Accomplishments

- ▶ GSA supported FEMA and the NCS during the 2007 calendar year for disaster relief and training efforts.
- ▶ GSA provided the NCSRM/FECC from almost all the regions to staff Regional Response Coordinating Centers, Joint Field Offices, and State Emergency Operations Centers as needed.
- ▶ GSA provided support for Continuity of Operations Planning and NS/EP exercises throughout the country and provided telecommunications support to FEMA for declared disasters.
- ▶ GSA continued FAS-ITS participation in the National Defense Executive Reserve which is a program for recruiting and training experienced business executives and other civilian personnel to serve in key government positions during periods of national emergency. Reservists augment the FAS-ITS staff or other Federal departments and agencies when organizations must rapidly mobilize to respond to national security emergencies.
- ▶ FAS-ITS participated in activities of the Committee on National Security Systems, the Priority Service Working Group, the Joint Telecommunications Resources Board, Continuity of Operations and Continuity of Government exercises, the Continuity Communications Working Group, the Communications Government Coordinating Committee, the National Coordinating Center, the National Security Information Exchange, the NCS Committee of Principals and the NCS Council of Representatives.

## Other Significant Activities

FAS-ITS is presently engaged in modifying current IT and Network Services contracts to include any anticipated needs that may arise during emergency situations and ensure these contracts are readily accessible to FEMA and the NCS to facilitate rapid recovery efforts.

FAS-ITS continues to provide industry components, Federal departments and agencies current information regarding available services, including disaster support, contingency planning, and continuity of operations services through participation in a number of multi-agency committees, working groups, and the GSA website (<http://www.gsa.gov>).



# National Aeronautics and Space Administration (NASA)

## NS/EP Telecommunications Mission

The National Aeronautics and Space Administration (NASA) shall (pursuant to an Executive Order dated February 28, 2003) coordinate with the Secretary of Homeland Security to prepare for use, maintenance, and development of technologically advanced aerospace and aeronautics-related systems, equipment, and methodologies applicable to national security emergencies.

## Current/Ongoing NS/EP Telecommunications Activities

NASA continues to support the National Communications System in achieving its assigned missions and the successful accomplishment of national-level programs approved by the White House. This includes Telecommunications Service Priority (TSP), Wireless Priority Service, and the National Telecommunications Management Structure.

NASA also continues to actively participate and manage NASA resources in the Shared Resources High Frequency Radio Program, Government Emergency Telecommunications System, the Network Design and Analysis Capability, and the Interagency Committee on Search and Rescue.

## NASA/EP Telecommunications Assets

NASA Integrated Services Network supports both spaceflight critical communication services and day-to-day administrative and scientific applications within the Agency, its contractor and research partners, and international space partners. The telecommunications services provided are primarily obtained through the General Services Administration contracts with the commercial sector.

NASA Space Network is a constellation of geostationary Tracking and Data Relay Satellites providing almost uninterrupted communications with NASA's Earth-orbiting spacecraft, human-tended vehicles, and other supported customer satellites.

NASA Deep Space Network supports deep space interplanetary, high-Earth orbiting spacecraft, and radio science missions.

NASA Near Earth Network (NEN) supports Low-Earth orbiting space flight missions. NASA obtains a significant portion of NEN services from the commercial market.

## NASA Significant Accomplishments

- ▶ Participated in Sharers Exercises from multiple continental U.S.-dispersed NASA facilities; and
- ▶ Participated in TSP.



# Nuclear Regulatory Commission (NRC)

## NS/EP Telecommunications Mission

The Nuclear Regulatory Commission (NRC) is responsible for ensuring adequate protection of the public health and safety, the common defense and security, and the environment with respect to the use of nuclear materials for civilian purposes in the United States. Activities licensed and regulated by the Commission include commercial nuclear power reactors; non-power research, test, and training reactors; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transportation, storage, and disposal of nuclear materials and waste.

The Commission's national security and emergency preparedness (NS/EP) telecommunications provide for highly reliable connectivity between the NRC emergency operations center and operating nuclear power plant control rooms, various emergency operations facilities, and regional incident response centers. This connectivity provides a means for immediate notification to the NRC Operations Center of unusual occurrences and communicating relevant information during accidents/events at NRC licensed facilities.

## Current/Ongoing NS/EP Telecommunications Activities

The NRC supports National Communications System (NCS) NS/EP programs and remains active in the NCS Committee of Principals and Council of Representatives activities. The systems and programs used in support of NS/EP telecommunications include Emergency Telecommunications System (ETS), Satellite Phones, Wireless Priority Service (WPS), Government Emergency Telecommunications System (GETS), Critical Warning Infrastructure Network (CWIN), Secure Communications, and Secure Video Teleconferencing System.

Presently, 51 NRC-licensed nuclear facilities use ETS with Telecommunications Service Priority through FTS 2001 and 23 facilities use private corporate systems. Satellite phones are used by headquarters and regional, as well as resident, inspectors at every U.S. nuclear power plant. WPS is used on cell phones assigned to key agency staff and members of the NRC incident response organization with continuity responsibilities. GETS is used by agency staff to enhance access to long distance service. A CWIN terminal and telephone is maintained in the Headquarters Operations Center. Secure communications is maintained between the

agency and licensed nuclear facilities and Secure Video Teleconferencing is used in the Headquarters Operations Center and at all of the NRC Regional Incident Response Centers. Monthly tests of all communications assets are conducted from the Headquarters Operations Center and its backup location. NRC staff test GETS, Satellite phones, and WPS quarterly.

## NRC Significant Accomplishments

- ▶ Installed a Defense Red Switch Network system at Headquarters and backup location;
- ▶ Installed an Federal Aviation Administration Domestic Events Network line at Headquarters and backup location;
- ▶ Initiated procurement of a web-based incident management tool to coordinate with other State and Federal agencies;
- ▶ Upgraded designated secure cell phones to meet NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, requirement;
- ▶ Purchased and deployed secure satellite phones to designated staff to meet NCS Directive 3-10 requirement.

# National Telecommunications and Information Administration (NTIA)



## NS/EP Telecommunications Mission

The National Telecommunications and Information Administration (NTIA) national security and emergency preparedness (NS/EP) mission, as tasked under Executive Orders 12046, 12472, and 12656, includes serving as the Executive Branch telecommunications policy adviser to the President, serving as the manager of Federal Government use of the radio frequency spectrum under all conditions, and serving as a member of the Joint Telecommunications Resource Board (JTRB). Thus, among other things, NTIA advises and assists the President in the administration of a system of radio spectrum priorities for those spectrum-dependent telecommunications resources of the Federal Government that support NS/EP functions.

## Current/Ongoing NS/EP Telecommunications Activities

The NTIA Office of Spectrum Management (OSM) continues its efforts to develop a U.S. spectrum policy for the 21st century in response to the President's Spectrum Policy Initiative of May 2003. Part of the OSM vision is to use information technology (IT) to automate the spectrum management business processes and to be more effective and efficient in all Federal spectrum use including NS/EP applications. Specific examples of activities in this regard include the following:

- ▶ Using an OSM Enterprise Architecture Council to identify IT requirements of the Federal spectrum management community and appropriate plans to satisfy those requirements, for example, this year NTIA developed the Federal Spectrum Management System (FSMS) Transition Plan.
- ▶ Continuing efforts under a memorandum of agreement with the Federal Communications Commission and the Department of Defense to leverage available resources in developing common spectrum management systems and approaches as appropriate.
- ▶ Acquiring the necessary IT infrastructure equipment to establish the new FSMS environments.
- ▶ Continuing to plan and implement a phased series of FSMS improvements.
- ▶ Continuing to develop, field, and maintain several spectrum management automation tools for use by Federal spectrum managers to more effectively

manage use of the radio frequency spectrum during NS/EP and normal conditions.

In addition, NTIA is continuing to:

- ▶ Serve as a non-resident member of the National Communications System (NCS) National Coordinating Center.
- ▶ Participate in various NS/EP support activities relative to national emergency management and continuity of Government as well as agency continuity of operations.
- ▶ Participate in various activities of the President's National Security Telecommunications Advisory Committee.
- ▶ Serve as Co-Chair of the Government Emergency Telecommunications Service (GETS)/Wireless Priority Service (WPS) User Council, participate in Council endeavors, and provide GETS/WPS user authorizations to all new NTIA emergency employees.
- ▶ Serve as a Government member of the NCS Telecommunications Service Priority Oversight Committee.
- ▶ Participate in NCS Committee of Principals (COP) and Council of Representatives activities and endeavors to include the NCS COP Priority Services Working Group and Communications Dependency on Electrical Power Working Group.
- ▶ Participate in the NCS SHARED RESOURCES (SHARES) High Frequency (HF) Coordination Network and NCS SHARES HF Interoperability Working Group activities.

## Significant Accomplishments

- ▶ Fully supported the NCS relative to the National Response Framework Emergency Support Function #2 (ESF #2), Communications, for example, five NTIA personnel actively participated in the ESF #2 Spring Conference in June 2007.
- ▶ Coordinated and assisted in developing the spectrum management portions of numerous State and regional emergency communications plans (ECPs) such as the Gulf Coast ECP and the Federal Frequency Quick Guide for AL-LA-MS Coastal Counties.





- ▶ Published the report “A Public Safety Sharing Demonstration” under the President’s Spectrum Policy Initiative.
- ▶ Continued development of the Federal Strategic Spectrum Plan.
- ▶ Completed a major Department-wide project to enhance continuity communications capabilities by providing authorized users access to the Secret Internet Protocol Router Network, and initiated another project to provide authorized users access to the Joint Worldwide Intelligence Communications System.
- ▶ Participated in Exercise PINNACLE 2007 by activating the primary NTIA alternate operating facility, deploying over 50 percent of NTIA emergency employees as exercise participants, and testing all interoperable communications with partner agencies.
- ▶ Regularly participated in quarterly Title Globe exercises to test NTIA interoperable communications at its primary and alternate operating facilities.
- ▶ Participated as a principal member of the JTRB and its senior staff working group.
- ▶ Represented the U.S. Government on many spectrum policy matters at various meetings of International Telecommunication Union and the Inter-American Telecommunication Commission as well as in bilateral discussions with Canada and Mexico regarding coordination of spectrum use in border areas.



# National Security Agency (NSA)

## NS/EP Telecommunications Mission

The National Security Agency (NSA) mission supports the critical intelligence needs of the Department of Defense (DOD) and national security community, and provides technical support necessary to develop and maintain the security and protection of national security and emergency preparedness (NS/EP) telecommunications.

### Information Technology and Information Assurance

Within NSA, several organizations share responsibility in supporting NS/EP related activities: National Information Assurance Research Laboratory (NIARL), Information Assurance (IA) worldwide enterprise, and Technology Directorate (TD).

- ▶ The NIARL conducts and sponsors research in the technologies and techniques needed to secure U.S. national security systems, to include cryptography, high-confidence software and systems, authentication, high speed security solutions, secure wireless multimedia, secure operating systems and network management, privilege management, and controlled sharing.
- ▶ The IA worldwide enterprise partners with academia, industry, and Government to provide IA solutions in an effort to keep U.S. national security systems safe from harm. This mission involves detecting and reporting on cyber threats, as well as making encryption codes to securely pass information among systems. It includes embedding IA measures directly into the DOD's emerging Global Information Grid (GIG); developing secure audio and video communications equipment; developing tamper protection products; and providing trusted microelectronics products.
- ▶ The TD plans and operates the telecommunications systems and networks that link NSA elements worldwide, as well as provides connectivity to other Government services.

In accordance with its National Security Telecommunications and Information Systems Manager responsibilities under National Security Directive 42, the NSA provides IA products and services that are applicable across the Government for the protection of national security systems. IA activities include close working relationships with the National Institute of Standards and Technology (NIST), the

Department of Homeland Security, and other entities with IA responsibilities. IA should be an integral part of any continuity plan and/or recovery in the event of a national crisis or emergency. In support of these roles, the NSA is maintaining a leadership role in the following activities:

### Current/Ongoing NS/EP Telecommunications Activities

#### NSA Commercial Solutions for NS/EP Telecommunications

- ▶ NSA is developing the High Assurance Platform (HAP) using commercial Trusted Computing Technologies to provide a higher assurance computing platform capable of connecting to multiple classified networks and supporting cross-domain data access. Release 1 of the HAP solution is being piloted at Special Operations Command and Navy in late 2008.

#### NSA Indications and Warning to NS/EP Telecommunications

- ▶ The NSA provides real-time global network awareness and threat characterization capabilities to forecast, alert, and guide risk mitigation and countermeasures in response to activities directed against U.S. national security systems. NSA activities include the discovery and reporting of possible malicious network behavior.
- ▶ The NSA provided expert assistance to the national security community regarding computer network defense. This was accomplished through unique, tailored, time-critical, and term reporting.

#### Cryptographic Modernization Initiative Supporting NS/EP Telecommunications

- ▶ The Cryptographic Modernization Initiative is a DOD-directed/NSA-led effort to transform and modernize capabilities for the 21st century. The initiative coordinates and oversees modernization by replacing an aging cryptographic product inventory, meeting increased interoperability needs, keeping pace with the evolution of information technology, and achieving objectives needed to enable the IA component of the DOD GIG architecture.



### Electronic Key Management System (EKMS) for NS/EP Telecommunications Systems

- ▶ The EKMS is a multi-tiered, distributed key management system designed to generate and distribute electronic key and automate the management of physical key and cryptographic equipment.
- ▶ EKMS Phase 5 capabilities have enhanced keying material accountability and management to the local operational units.
- ▶ Additionally, EKMS capabilities enhancements have improved the ability to respond to dynamic interoperability requirements as well as automating the rekey process for some additional secure communication products.

### Physical to Electronic Transition of Keying Material Supporting NSA/EP Telecommunications

- ▶ Reduction initiatives affecting all NSA customers who use physical cryptographic key material have been put in place. Sunset dates identifying the termination of production for punched tape key and key provided on floppy disks have been released. Electronic key solutions are available for these physical key items. This will allow increased net-centric operations and efficiency. NSA customers have initiated efforts to comply. Further reductions of other physical key products are being evaluated.

### DOD Identity Assurance/Public Key Infrastructure

- ▶ In support of DOD, NSA is managing DOD's Identity Assurance efforts, which will help facilitate greater information sharing among and between DOD and its constituents. Using Homeland Security Presidential Directive 12 as the foundation, the activity leverages DOD's Public Key Infrastructure program to issue logical identity credentials to all DOD personnel. It associates individuals with attributes and then defines privilege rights to access information. One area where the potential of the capability will be exercised is with first responders.

### Enterprise Security Management (ESM)

- ▶ Identified by IA Directorate Senior Leadership as a strategic initiative, ESM provides the foundation for ensuring the trust and integrity of enterprise information, and allows flexible and fine-grained control of information sharing in the GIG. ESM comprises the systems, processes, and the personnel required to order, create, disseminate, modify, suspend, and terminate management control to provision and operate IA services processes and devices across the enterprise. ESM is a collaborative effort of systems engineers, program managers, contractors, and the Defense Information Systems Agency (DISA) working to establish the following nine capabilities of ESM:

1. Identity Management
2. Attribute Management
3. Credential Management
4. Privilege Management
5. IA Metadata Management
6. Digital Policy Management
7. IA Configuration Management
8. IA Audit Management
9. Cryptographic Key Management

As a first step toward implementation of ESM, a combined team of diverse capabilities is currently developing a pilot that features one of the nine ESM capabilities: Privilege Management. The Privilege Management Pilot will be launched in the operational space of an identified Combatant Command customer in September 08. Joint DISA and NSA initiatives addressing Enterprise-wide Privilege Management, IA Configuration Management and IA Audit Log Management commence next year.

### Security Assessments Supporting NS/EP Telecommunications

- ▶ The NSA continues to perform security assessments to evaluate the security of national security customers' information systems and operations. Security assessments can include IA assessments, network technology analysis, technical security evaluations, Technical Security Countermeasures Operations, and TEMPEST services. Technical advice and assistance in support of assessments and evaluations within annual exercises have also been provided.



## IA Services Supporting NS/EP Telecommunications

- ▶ The Federal Desktop Core Configuration (FDCC) is a Government standard desktop that has been co-developed by Microsoft, NSA, DISA, NIST, and the military services, which has been mandated for use across the U.S. Government by the Office of Management and Budget. The FDCC is based on work done by NSA/Vulnerability Analysis Operations, DISA, and the services to develop standard DOD desktops for the Windows XP and Vista operating systems.
- ▶ The Cyber Defense Exercise (CDX) took place in April 2008. For the second consecutive year, special congratulations went out to the U.S. Military Academy at West Point as the winner of the annual event. CDX tested and evaluated the IA knowledge of cadet and midshipmen enrolled in computer science programs at each of the Armed Forces Service Academies. Overall, cadets and midshipmen did an outstanding job securing and defending their networks.

## Global Information Grid (GIG)

- ▶ The NSA's Enterprise IA Systems Engineering effort leads the Community in operationalizing the enterprise level IA architecture strategy for the DOD's GIG. The goal is to enable Defense-in-Depth to achieve an assured, integrated, and survivable GIG enterprise. To move towards that goal, NSA partnered with the DISA to define the appropriate network defense protections to be implemented throughout the GIG. NSA has also taken the lead on defining IA metadata standards, which will increase the security of classified networks by supporting higher granularity security policy enforcement and secure information sharing. NSA is producing an Alignment Framework for GIG IA structured around the proposed Committee for National Security Systems 1253 Security Controls Catalog. This allows clients to independently plan and assess GIG IA architectural alignment, assisting with Clinger-Cohen Act compliance and certification.

## Information Assurance (IA) Capabilities

- ▶ NSA's Initial Capabilities Document (ICD) for the GIG IA was approved by the DOD's Joint Requirement Oversight Council (JROC) in early 2007. The GIG IA ICD articulates a universal set of capabilities that

are essential independent of network architecture and user community, and thus apply equally well to intelligence community (IC) networks. These IA capabilities were integrated into NSA's Unified Cryptologic System Joint Capabilities Document, which has been formally vetted by both the JROC and the IC's mission Review Board (MRB). NSA is similarly integrating these IA capabilities into five mission-related ICDs currently under development. The MRB has expressed interest in formal consideration of the IA capabilities described in the GIG IA ICD. In preparation for this formal review, NSA will crosswalk the fifteen IA capabilities against the three IC mission scenarios to demonstrate that they are both necessary and sufficient to satisfy the IC's IA needs. The establishment of a common set of defined IA capabilities agreed upon by the DOD and the IC is fundamental to achieving compatible and interoperable IA solutions for the nation's assured information sharing and network defense needs.

## Cross Domain Solutions (CDS)

- ▶ The NSA has a long history of helping national security systems customers resolve assured information sharing problems between network domains. In an effort to help unify cross domain standards between the IC and the DOD, NSA has worked closely with the Unified Cross Domain Management Office in the area of certification and accreditation policy and testing procedures. These policies and procedures were reviewed by NSA subject matter experts, and comments provided to ensure completeness. This information was also shared within the 5-Eyes community (Australia, Canada, Great Britain, New Zealand, and the United States) to get comments and expertise from our partners. The extensive review of these policies and procedures will ensure that the Defense and ICs gain the benefit of a common set of cross domain criteria, which will be necessary in their quest for information sharing at the enterprise level.

## Vulnerability Analysis and Operational Assessments

- ▶ The NSA provides vulnerability analysis and operational assistance to the national security community regarding computer network defense. These activities were accomplished through unique leadership and technical expertise in the areas of operations, technology analysis, community coordination, policy, as well as analysis and

reporting. NSA provides, through close partnership with DOD and national security customers, operational, crisis, and exercise planning to ensure that cyber defense activities and responses promoted good actionable countermeasures and recovery. These assessments provided a unique look at U.S. Government systems, operations, personnel, and current technology, which enabled the protection and defense of information by mitigating risks. Expert operational analysis and guidance is sustained through state-of-the-art technology evaluations covering a wide range of communication components, network applications, and software applications.







# Federal Reserve Board (FRB)

## NS/EP Telecommunications Mission

The Federal Reserve Board's (FRB) national security and emergency preparedness (NS/EP) responsibilities relate to the maintenance of the national economic posture, and in particular: the operation and liquidity of banks; the maintenance of national monetary, credit, and financial systems; and the maintenance and restoration of stable and orderly markets. The FRB considers essential services and systems related to the national economic posture to include: critical funds transfer systems (wholesale/large-value payment systems); securities and derivatives clearing and settlement systems; supporting communications systems and service providers; and key financial market trading systems and exchanges.

## Telecommunications Staff Organization

The Associate Director in the Board's Division of Reserve Bank Operations and Payment Systems has responsibility for oversight of the Federal Reserve Banks' telecommunications services and serves as a liaison member on the National Communications System (NCS) Committee of Principals.

## Current/Ongoing NS/EP Telecommunications Activities

The FRB supports NCS initiatives designed to provide essential telecommunications services needed to maintain the nation's financial telecommunications infrastructure and payment systems. The FRB continues to sponsor Telecommunications Service Priority (TSP) assignments for essential telecommunications services supporting large-value payment systems, large-value clearing and settlement systems, major financial services exchanges and utilities, Federal Reserve open market and foreign operations, and the automated auction processing system for Treasury securities. In addition, the FRB administers the TSP program for financial service organizations sponsored by the Securities and Exchange Commission (SEC), Office of the Comptroller of the Currency (OCC), Commodities and Futures Trading Commission (CFTC), National Credit Union Administration (NCUA) Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS).

The FRB sponsors the Government Emergency Telecommunications Service (GETS) and the Wireless Priority Service (WPS) for Federal Reserve Banks, depository institutions, key participants in the nation's

payment systems, and those foreign central banks that are critical to the maintenance of the nation's economic posture.

The FRB continues to provide outreach to those financial institutions that support NS/EP functions and actively participates in NCS initiatives to enhance the resiliency of the nation's financial telecommunications infrastructure.

## FRB Significant Accomplishments

The FRB focused its NS/EP activities on its sponsorship role for assigning TSP status, primarily at restoration level four, to essential telecommunications services under criteria it adopted in 1993 and expanded in 2002. The FRB continues to sponsor TSP assignments for the following:

- ▶ Circuits used for Fedwire funds transfer and securities transfer services, including access circuits to the Fedwire network from depository institutions that engage in large-dollar Fedwire transactions;
- ▶ Voice and data circuits supporting Federal Reserve open market and foreign operations, the automated auction processing system for Treasury securities, and critical central bank functions;
- ▶ Circuits used by other payment systems (such as, the Society for Worldwide Interbank Financial Telecommunications and the Clearing House Interbank Payments System) that meet the FRB's eligibility criteria;
- ▶ Circuits used for large-dollar clearing and settlement services, including access circuits to the Federal Reserve's net settlement service, the networks of Automated Clearing House (ACH) operators, the Continuous Linked Settlement (CLS) bank, and other qualifying financial service utilities;
- ▶ Circuits used by ACH operators and the CLS bank that meet the FRB's eligibility criteria;
- ▶ Circuits connecting customers of sponsored payment system, foreign exchange, and clearing and settlement utilities that meet the FRB's eligibility criteria;
- ▶ Circuits used by capital and futures exchange utilities and key participants that meet the SEC and CFTC eligibility criteria;



- ▶ Circuits used by market data providers that supply critical information needed by financial institutions; and
- ▶ Circuits used by the World Bank to ensure continuity of operations.

By the end of this fiscal year, there will be approximately 5,000 active TSP assignments including circuits directly sponsored by the FRB as well as those circuits administered for the SEC, OCC, CFTC, NCUA, FDIC and OTS.

The FRB has implemented GETS across the Federal Reserve System to support communications within the Federal Reserve System and with depository institutions in the event of a disaster or communications disruption. In December 2002, the FRB began sponsoring other key participants in the nation's payment systems. In fiscal year 2008, the Federal Reserve participated in the Financial and Banking Information Infrastructure Committee (FBIIC) GETS Pilot Program. The pilot program was conducted to foster awareness and evaluate distributing GETS cards as a preemptive tool to supplement preparedness for the financial services sector for national emergencies and natural disasters. The program focused on financial organizations in the hurricane regions of the southeastern United States. The Federal Reserve sponsored 14 private institutions as a result of the pilot program activities. As a result of the FBIIC GETS Pilot Program and other Federal Reserve sponsored institutions, the Federal Reserve will have sponsored a total of approximately 74 institutions for GETS by the end of this fiscal year.

During the last fiscal year, the FRB continued to participate in the evolution of the WPS program. The FRB has sponsored approximately 35 institutions for WPS.

### National Diversity Assurance Initiative/Diversity Assurance Analysis

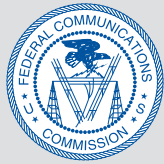
In 2005 and early 2006, the National Diversity Assurance Initiative (NDAI), led by the Alliance for Telecommunications Industry Solutions Chief Information Officer's Council and the Federal Reserve Board, evaluated the problem inherent in assuring physical diversity of NS/EP financial service circuits in a multi-carrier environment. At the completion of the Assessment Phase, the team concluded that end-to-end multi-carrier circuit diversity assurance currently cannot be conducted in a scalable manner. The cost and level of manual effort required were comparable

to the assessment step and demonstrated that an ongoing program for end-to-end multi-carrier circuit diversity assurance, as it exists today, cannot be offered as a widely available commercially viable product.

The NDAI team recommended a follow-up effort to determine more accurately the requirements for providing an automated end-to-end diversity assurance solution in a multi-carrier environment. In early 2007, the NCS initiated the Diversity Assurance Analysis (DAA) to analyze several models for carriers to establish methods to record circuit diversity data and to exchange diversity data between carriers, when applicable. In May 2007, a financial services subject matter experts advisory group, comprised of the Federal Reserve, Bank of America, and NYSE/EuroNext, sent a joint letter to the NCS that identified several issues and concerns with the draft DAA report that raised possible deficiencies in the ability of carriers to comply with the 1988 FCC Order establishing TSP. The Federal Reserve also raised these concerns regarding carrier support of TSP, to the FCC.

### Pandemic Flu Preparations

The Federal Reserve Board has developed contingency plans to continue the operation of the NS/EP priority telecommunications programs in the event of a pandemic flu outbreak. The plan incorporates the training and equipping of staff located in disparate regions of the country. In early 2008, The Federal Reserve worked with Treasury to hold an "International Symposium on the U.S. Financial Services Sector Pandemic Flu Exercise of 2007" that was held on January 28-29, 2008.



# Federal Communications Commission (FCC)

## NS/EP Telecommunications Mission

The Federal Communications Commission's (FCC) national security and emergency preparedness (NS/EP) responsibilities include the following:

- ▶ Developing policies and promulgating regulations for effective communications through wire and radio for the national defense and promotion of safety of life and property.
- ▶ Evaluating and strengthening measures for protecting and preserving critical communications infrastructure and associated systems.
- ▶ Facilitating rapid restoration of critical communications infrastructure and systems following disruptions, regardless of the cause.
- ▶ Participating in international organizations and conferences to coordinate global communications issues and promote the Nation's interests.
- ▶ Coordinating with industry and other federal, tribal, state, and local entities regarding public safety, homeland security, and disaster preparedness and response.
- ▶ Serving as the Federal collector of real-time communications infrastructure and service outage and restoration information from wireline, wireless, cable, broadcast, satellite, and other communications service providers.
- ▶ Coordinating with the National Telecommunications and Information Administration in assigning radio frequencies, determining priorities for the use of those frequencies, and managing the use of the same.
- ▶ Providing expert technical advice to policymakers on wireless and wireline matters.
- ▶ On February 6, 2008, the FCC hosted a Summit on 9-1-1 Call Center operations. The Summit addressed disaster preparation and response for 9-1-1 Call Centers and the evolution of 911 toward next generation networks (NGN) architectures.
- ▶ In April 2008 the FCC sought comments, analysis, and information related to 911 calls from non-service initialized phones.
- ▶ In April 2008, the FCC updated functionality of the Disaster Information Reporting System (DIRS) to provide for graphical presentation of situational awareness information on a discrete basis (such as, maps showing the locations of failed or impaired telephone switches, broadcast stations, and cellular switches).
- ▶ DIRS is a voluntary web-based system that communications companies use to report infrastructure status. DIRS, which was launched in September of 2007, has contact information for over one thousand companies. In May of 2008, DIRS was used as part of the National Level Exercise to simulate hurricane impact on the communications sector.
- ▶ In May 2008, the FCC hosted an Emergency Alert System (EAS) Summit addressing current EAS architecture, operations, and NGN transitional issues. The FCC is exploring these issues in an on-going EAS rulemaking proceeding.
- ▶ On May 14, 2008, the FCC issued notice of its intent to move forward with the "D Block" of spectrum and the creation of a nationwide interoperable public safety broadband network. Public comment is due during the summer of 2008.
- ▶ In May of 2008, three senior FCC staff members and two observers attended Federal Emergency Communications Coordinator cadre training.

## Current/Ongoing NS/EP Communications Activities

- ▶ On November 20, 2007, the FCC released set benchmarks for measuring wireless location accuracy (Enhanced 911 or E911). Although the D.C. Circuit stayed this action, the proceeding remains open with work being done on outstanding issues.
- ▶ The FCC is finalizing development of a deployable spectrum analyzer that will scan broadcast and public safety frequencies to map operational status. Nicknamed Project Roll Call, the FCC will send communications engineers and the device along with the Federal Emergency Management Agency's (FEMA) disaster strike teams to develop situational awareness.



- ▶ In June of 2008, in support of disaster operations in Cedar Rapids, Iowa, the FCC deployed a communications engineer to resolve interference to FEMA's satellite communications.
- ▶ In July of 2008, the FCC deployed two senior engineers (and had two on standby) to assist Emergency Support Function 2 (ESF #2) response in Texas following Hurricane Dolly's landfall.
- ▶ Beginning in July of 2008, 30 FCC staff members and senior leadership participated in ESF #2 training sessions; the FCC also provided subject matter expertise for ESF #2 job aids.

## NS/EP Telecommunications Mission

The U.S. Postal Service (USPS) delivers to every household and business in the United States (300 million people at 148 million homes, businesses and Post Office Boxes in every state, city, and town, and in Puerto Rico, Guam, the American Virgin Islands, and American Samoa). Every American has access to our products and services and pays the same postage rate for First-Class® Mail service regardless of geographic location. The USPS:

- ▶ Delivers 212 billion pieces of mail to over 148 million homes, businesses and Post Office boxes in virtually every state, city, and town in the country, including Puerto Rico, Guam, the American Virgin Islands, and American Samoa.
- ▶ Handles more than 46 percent of the world's card and letter mail volume—delivering more mail to more addresses and to a larger geographic area than any other postal service in the world.
- ▶ Is the second largest employer in the United States with nearly 685,000 career employees.
- ▶ Does not receive tax dollars for operations. We are a self supporting agency, using revenue from the sale of postage and products to pay expenses.
- ▶ Operates the largest civilian vehicle fleet in the world with more than 219,000 vehicles driving more than 1.2 billion miles each year and using 121 million gallons of fuel.
- ▶ Provides services at:
  - More than 27,800 vending machines
  - Nearly 33,000 commercial retail outlets
  - Nearly 17,000 banking and credit union ATMs
  - 2,500 Automated Postal Centers®
- ▶ Has annual operating revenue of nearly \$75 billion.
- ▶ Has one of the largest e-mail systems, delivering more than 13 million emails a day with an average delivery time of less than five minutes.

- The USPS intranet is the largest in the world connecting more than 28,000 locations to critical business systems 24 hours a day, 365 days a year.

## Benefits

Information Technology (IT) is dedicated to helping the Postal Service improve service and operations through technology. In the telecommunications area, IT has equipped key personnel with the tools necessary to continue operations in the event of a national or local emergency or disaster. IT has employed National Communications System (NCS) tools and offerings such as the Government Telecommunications System (GETS) and Wireless Priority Service (WPS) to many key personnel in order to maintain vital communications and services to the public.

IT has also upgraded all of the USPS Large Private Branch Exchange (PBX) Telephone Systems throughout the country. IT has also refreshed many Key Telephone Systems at smaller Postal Service facilities throughout the country.

The Postal Service has not been assigned any specific national security and emergency preparedness (NS/EP) telecommunications responsibilities in the event of a national emergency or other declared disaster. Therefore, the Postal Service designs, engineers and develops telecommunication systems, services and solutions to support day to day organizational, administrative, and operational mission requirements.

## USPS Significant Accomplishments

### Upgrading the Telecommunications Infrastructure (Voice)

After the extensive improvements and upgrades to the USPS Data Network in fiscal year (FY) 2006, the Postal Service moved to upgrade the voice communications network throughout the country. The two major types of telephone systems, PBX and Key Telephone Systems were targeted for improvements.

### Private Branch Exchange Telephone System (PBX)

The Postal Service standard PBX is a Nortel. There are various models that are equipped throughout the larger offices within the system. Options 11, 61, and 81 are the models that are deployed and were targeted for upgrading.







The upgrading of these systems included the latest vintage software as offered by Nortel along with improvements in hardware and adjunct systems. All PBX's have integrated voice mail, Uninterruptible Power Supplies, administrative terminal access and call accounting. Furthermore, the upgrade effort included hardware and software for these systems to operate in a Voice over Internet Protocol (VoIP) environment. Presently, these systems are operating with conventional Digital Primary Rate Interface trunks for commercial and within network calling.

### Key Telephone Systems

The Postal Service standard Key System is an Avaya. These systems are sized depending on the amount of handset required by the facility. Each system is equipped with one cordless telephone to offer mobility for the supervisor. Some systems have voice mail and Uninterruptible Power Systems. These systems are connected into the Public Switched Network via conventional telephone lines from the Local Exchange Carriers.

In FY 2008, USPS has replaced more than 250 key telephone systems in Main Post Offices, Stations and Branches throughout the Postal Service. This effort was designed to update systems that were over ten years old and no longer adequate for the activities of a 21st Century facility. The replacements included, in some cases, new improved paging systems as well as wiring in order to improve employee communication and customer service.

### PBX Security

All PBX's in the USPS have been configured to limit the amount of access local personnel have to make changes to the system. The PBX's are locked down to not allow trunk to trunk transfers that can open the systems up to hackers. The PBX's are also monitored for calling patterns that are unusual that would indicate fraudulent or criminal activity maybe occurring.

All PBX's are monitored at a Central Network Operations Center so that any alarms or malfunctions can be acted on immediately. In addition, Postal executives are advised in real time about the state of these PBX's so that pro-active plans may be issued to advise employees and business partners of any outage or malfunction.

### NCS Directive 3-10

The USPS has several of the communications requirements as identified in NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, and has a budget and program plan that will enable USPS to move forward in implementing NCS Directive 3-10.

### Wide Area Network Upgrades

Since the beginning of this fiscal year we have upgraded the telecommunications service at numerous Postal facilities. Most of the facilities moved from a low speed (VSAT, 56k frame, DSL) connection to a 768k dedicated service with fixed performance service level agreements. This increase in service level has reflected in increased computer performance at Postal locations nationwide.

### Conversion from Dial up to Broadband

The USPS has additionally increased the level of network capacity and security at all upgraded sites by converting from dial and installing a managed Virtual Private Network (VPN) firewall router at each location—thus protecting USPS computer assets from any malicious internet activity. Total number of broadband enabled locations now reaches over 8,000 USPS locations; 2,236 sites were upgraded in FY 2006.

There are currently 7,500 VPN/Firewall Routers deployed and managed by USPS not including the critical back-office VPN and security gear that make this huge web of nationwide VPN sites possible.

### Dial up to Broadband Stats Recap

- ▶ Total Number of dial-up sites upgraded to Broadband: 8,000 and growing
- ▶ Broadband upgrades in the last two years: 2,236
- ▶ Total Number of VPN routers deployed and managed internally by USPS: 7,500 and growing
- ▶ Consolidated five broadband providers into just two providers thus simplifying troubleshooting and problem resolution.



### Centralized Cellular Services Management

The USPS has centralized cellular services management in order to reduce costs, enhance reliability, and to improve accountability. This effort has resulted in \$8 million in savings by eliminating unused devices and placing devices into a negotiated national minute pooling plan with the major cellular providers throughout the country. The average monthly recurring cost of cellular services has dropped a total of 30 percent this fiscal year. Providing Blackberry devices and Broadband Cellular technology to key employees within the management structure has allowed for the on-line managers to react promptly to changes in the environment and staffing in order to meet critical goals and objectives. It also allows for the user to have access to data and to communicate with parties internal and external for mission vital applications.



## NCS-Related Acronyms

## A

<b>ACH</b>	Automated Clearing House
<b>ACR</b>	Alternate Carrier Routing
<b>AES</b>	Advance Encryption Standard
<b>AFCEA</b>	Armed Forces Communications and Electronics Association
<b>AFT</b>	Assured File Transfer
<b>AGG</b>	Alert Gateway Group
<b>ANSI</b>	American National Standards Institute
<b>AOF</b>	Alternate Operating Facility
<b>ART</b>	Analysis Response Team
<b>ASD (HD)</b>	Assistant Secretary of Defense for Homeland Defense
<b>ASH (NII)</b>	Assistant Secretary of Defense for Networks and Information Integration
<b>ATG</b>	Advanced Technology Group
<b>ATIS</b>	Alliance for Telecommunication Industry Solutions
<b>ATO</b>	Authority to Operate

## B

<b>BCIS</b>	Bureau of Citizenship and Immigration Services
<b>BFEM</b>	Budget Formulation and Execution Manager System
<b>BLADE</b>	Biometric Logical Access Development and Execution Program
<b>BMC</b>	Beltsville Management Center
<b>BPD</b>	Bureau of Public Debt
<b>BRI</b>	Basic Rate Interface
<b>BRM</b>	Business Reference Model

## C

<b>C4</b>	Command, Control, Communications, and Computer Systems Directorate
<b>C&amp;A</b>	Certification and Accreditation
<b>CA</b>	Certification Authority
<b>CAA</b>	Controlled Access Area
<b>CAB</b>	Collaborate Access and Browse
<b>CALEA</b>	Communications Assistance for Law Enforcement Act
<b>CCA</b>	Continuity Communications Architecture
<b>CCPC</b>	Civil Communications Planning Committee
<b>CDC</b>	Center for Disease Control

<b>CDEP WG</b>	Communications Dependency on Electric Power Working Group
<b>CDFI</b>	Community Development Financial Institution
<b>CDMA</b>	Code Division Multiple Access
<b>CDS</b>	Cross Domain Solutions
<b>CDX</b>	Cyber Defense Exercise
<b>CEP</b>	Civil Emergency Planning
<b>CEPTAG</b>	Civil Emergency Planning Telecommunications Advisory Group
<b>CFIUS</b>	Committee for Foreign Investment in the U.S.
<b>CFTC</b>	Commodities and Futures Trading Commission
<b>CGCC</b>	Communications Government Coordinating Council
<b>CI</b>	Critical Infrastructure
<b>CIA</b>	Central Intelligence Agency
<b>CI/KR</b>	Critical Infrastructure/Key Resources
<b>CIO</b>	Chief Information Officer
<b>CIP</b>	Critical Infrastructure Protection
<b>CIPAC</b>	Critical Infrastructure Protection Advisory Committee
<b>CLS</b>	Continuous Linked Settlement
<b>CMN</b>	Crisis Management Network
<b>CMO</b>	Coordination and Management Office
<b>CMS</b>	Commercial Mobile Service
<b>CMSAAC</b>	Commercial Mobile Service Alert Advisory Committee
<b>CNSS</b>	Committee for National Security Systems
<b>COOP</b>	Continuity of Operations
<b>COP</b>	Committee of Principals
<b>COR</b>	Council of Representatives
<b>COTS</b>	Commercial Off-The-Shelf
<b>CP</b>	Contingency Planning
<b>CS&amp;C</b>	Cybersecurity and Communications
<b>CS&amp;T</b>	Cyber Security and Telecommunications
<b>CSCC</b>	Communications Sector Coordinating Council
<b>CSRIC</b>	Communications Security, Reliability, and Interoperability Council
<b>CSSP</b>	Communications Sector-Specific Plan
<b>CWIN</b>	Critical Warning Infrastructure Network

## D

<b>DAN</b>	Data Analysis Network
<b>DEA</b>	Drug Enforcement Administration
<b>DES</b>	Data Encryption Standard
<b>DHS</b>	Department of Homeland Security

<b>DHHS</b>	Department of Health and Human Services
<b>DIB</b>	Defense Industrial Base
<b>DIRS</b>	Disaster Information Reporting System
<b>DO</b>	Departmental Offices
<b>DOC</b>	Department of Commerce
<b>DOD</b>	Department of Defense
<b>DOE</b>	Department of Energy
<b>DOI</b>	Department of the Interior
<b>DOJ</b>	Department of Justice
<b>DOS</b>	Department of State
<b>DOT</b>	Department of Transportation
<b>DR</b>	Disaster Recovery
<b>DSD</b>	Deputy Secretary of Defense
<b>DSIE</b>	Defense Security Information Exchanges
<b>DS</b>	Diplomatic Security
<b>DSS</b>	Diplomatic Security Service
<b>DTCI</b>	Defensive Technical Counter-Intelligence
<b>DTS</b>	Digital Telecommunications Switching System

## E

<b>EAS</b>	Emergency Alert System
<b>EBS</b>	Emergency Broadcasting System
<b>ECITF</b>	Emergency Communications and Interoperability Task Force
<b>ECPs</b>	Emergency Communications Plans
<b>ECT</b>	Emergency Communications Teams
<b>ECT-F</b>	Emergency Communication Teams-Field
<b>ECT-N</b>	Emergency Communication Teams-National
<b>EKMS</b>	Electronic Key Management System
<b>EMC</b>	Emergency Management Centers
<b>EMP</b>	Electromagnetic Pulse
<b>E.O.</b>	Executive Order
<b>EOC</b>	Emergency Operations Center
<b>EOP</b>	Executive Office of the President
<b>ESF</b>	Emergency Support Function
<b>ETS</b>	Emergency Telecommunications System
<b>EU</b>	European Union
<b>EWB</b>	Emergency Wireless Protocol

## F

<b>FA</b>	Frequency Authorization
<b>FAS</b>	Federal Acquisition Service
<b>FBCA</b>	Federal Bridge Certificate Authority
<b>FBI</b>	Federal Bureau of Investigation
<b>FCC</b>	Federal Communications Commission

<b>FCO</b>	Federal Coordinating Officer
<b>FDIC</b>	Federal Deposit Insurance Corporation
<b>FEA</b>	Federal Enterprise Architecture
<b>FEB</b>	Federal Executive Branch
<b>FECC</b>	Federal Emergency Communications Coordinator
<b>FEMA</b>	Federal Emergency Management Agency
<b>FNARS</b>	FEMA National Radio System
<b>FOC</b>	Full Operational Capability
<b>FPIC</b>	Federal Partnership for Interoperable Communications
<b>FRB</b>	Federal Reserve Board
<b>FPKIPA</b>	Federal PKI Policy Authority
<b>FSMS</b>	Federal Spectrum Management System
<b>FTS</b>	Federal Technology Service (Section III)
<b>FY</b>	Fiscal Year

## G

<b>GCCC</b>	Government Communications Coordinating council
<b>GCS</b>	Global Communications Service
<b>GETS</b>	Government Emergency Telecommunications Service
<b>GFIRST</b>	Government Forum of Incident Response and Security Teams
<b>GIG</b>	Global Information Grid
<b>GITM</b>	Global IT Modernization
<b>GNO</b>	Global Network Operations
<b>GOTS</b>	Government Off-the-Shelf
<b>GPRA</b>	Government Performance and Results Act
<b>GSA</b>	General Services Administration
<b>GSM</b>	Global System for Mobile Communications

## H

<b>HAIPE</b>	High Assurance Internet Protocol Encryptor
<b>HCHB</b>	Herbert C. Hoover Building
<b>HF</b>	High Frequency
<b>HPM</b>	High Power Microwave
<b>HQ</b>	Headquarters
<b>HSDN</b>	Homeland Security Data Network
<b>HSPD</b>	Homeland Security Presidential Directive



## I

IA	Information Assurance
IAM	Initial Address Message
IC	Integration Contractor
IC	Intelligence Community
IES	Industry Executive Subcommittee
IMA	Individual Mobilization Augmentee
IMS	IP Multimedia Subsystem
INE	Inline Network Encryption
IOS	Interoperability Specification
IP	Internet Protocol
IR	Industry Requirements
IRAC	Interdepartment Radio Advisory Committee
IRM	Bureau of Information Resource Management
IRS-CI	Internal Revenue Service-Criminal Investigation
IS	Interoperability Specification
ISDN	Integrated Services Digital Network
IT	Information Technology
ITD	Information Technology Directorate
ITS	Integrated Technology Services
IWN	Integrated Wireless Network
I-WPS	Immediate Wireless Priority Service
IXC	Interexchange Carrier

## J

J6	Command, Control, Communications, and Computer Systems Directorate
JCG	Joint Contact Group
JFO	Joint Field Office
JTRB	Joint Telecommunications Resource Board
JUTNet	Justice Unified Telecommunications Network

## K

Kbps	Kilobit per second
KCP	Kansas City Plant

## L

LAN	Local Area Network
LEC	Local Exchange Carrier
LMR	Land Mobile Radio

LRTF  
LTO

Legislative and Regulatory Task Force  
Long-Term Outage

## M

MCO	Management Coordination Office
MERS	Mobile Emergency Response Support
MHD	Magneto Hydro Dynamics
MHz	Megahertz
MOA	Memoranda of Agreement
MRTD	Machine Readable Travel Document
MSC	Mobile Switching Center
MSF	MultiService Forum
MSO	Managed Service Offering
MXU	Multi-Exchange Units
MYSPM	Multi-Year Strategy and Program Management Plan

## N

NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center
NCCC	National Command and Coordinating Capability
NCCTF	National Coordinating Center Task Force
NCS	National Communications System
NCS D	NCS Directive
NCS D	National Cyber Security Division
NCSRM	National Communications System Regional Manager
NCUA	National Credit Union Administration
NDAC	Network Design and Analysis Capability
NECP	National Emergency Communications Plan
NECS	National Emergency Communications Strategy
NEF	National Essential Functions
NEMIS	National Emergency Management Information System
NEN	Near Earth Network
NGN	Next Generation Network
NGO	Non-Governmental Organizations
NIFC	National Interagency Fire Center
NIIF	Network Interconnection Interoperability Forum
NIST	National Institute of Standards and Technology

<b>NOAA</b>	National Oceanic and Atmospheric Administration	<b>PIN</b>	Personal Identification Number
<b>NOIWON</b>	National Operational Intelligence Watch Officers Network	<b>PIV</b>	Personal Identity Verification
<b>NOTF</b>	NSTAC Outreach Task Force	<b>PKI</b>	Public Key Infrastructure
<b>NPPD</b>	National Protection and Programs Directorate	<b>PMEF</b>	Priority Mission Essential Functions
<b>NRC</b>	Nuclear Regulatory Commission	<b>PMO</b>	Program Management Office
<b>NRF</b>	National Response Framework	<b>PPBE</b>	Planning, Programming, and Budgeting Execution System
<b>NSA</b>	National Security Agency	<b>PO</b>	Program Office
<b>NSC</b>	National Security Council	<b>PRM</b>	Performance Reference Model
<b>NSDD</b>	Network Security Decision Directive	<b>PSAP</b>	Public Safety Access Points
<b>NS/EP</b>	National Security and Emergency Preparedness	<b>PSHSB</b>	Public Safety and Homeland Security Bureau
<b>NSIE</b>	Network Security Information Exchange	<b>PSTN</b>	Public Switched Telephone Network
<b>NSPD</b>	National Security Presidential Directive	<b>PSWG</b>	Priority Services Working Group
<b>NSRA</b>	National Sector Risk Assessment		
<b>NSS</b>	National Security Systems		
<b>NSTAC</b>	The President's National Security Telecommunications Advisory Committee		
<b>NTIA</b>	National Telecommunications and Information Administration		
<b>O</b>		<b>R</b>	
<b>OA</b>	Operational Analysis	<b>R&amp;D</b>	Research and Development
<b>OCC</b>	Office of Comptroller of Currency	<b>R&amp;O</b>	Report and Order
<b>OCIO</b>	Office of the Chief Information Officer	<b>RCC</b>	Regional Communications Coordinator
<b>OEC</b>	Office of Emergency Communications	<b>RDM</b>	Route Diversity Methodology
<b>OEP</b>	Office of Emergency Preparedness	<b>RDTF</b>	Research and Development Task Force
<b>OHS</b>	Office of Homeland Security	<b>RDX</b>	Research and Development Exchange
<b>OMB</b>	Office of Management and Budget	<b>RFCs</b>	Request for Comments
<b>OMNCS</b>	Office of the Manager, National Communications System	<b>RL</b>	Richland Operations Office
<b>OPLAN</b>	Operation Plan	<b>RMOTC</b>	Rocky Mountain Oilfield Testing Center
<b>ORO</b>	Oak Ridge Office		
<b>OSD</b>	Office of the Secretary of Defense	<b>S</b>	
<b>OSM</b>	Office of Spectrum Management	<b>SAVCE</b>	Symantec AntiVirus Corporate Edition
<b>OSS</b>	Operations Services Staff	<b>SAVER</b>	Secure AntiVirus Equipment Refresh
<b>OSTP</b>	Office of Science and Technology Policy	<b>SBU</b>	Sensitive But Unclassified
<b>OTS</b>	Office of Thrift Supervision	<b>SEC</b>	Security and Exchange Commission
<b>P</b>		<b>SHARES</b>	Shared Resources
<b>P25</b>	Project 25	<b>SHARES-HF</b>	Shared Resources High Frequency Radio Program
<b>PAS</b>	Priority Access Service	<b>SMART</b>	State Messaging Archive Retrieval Toolset
<b>PBS</b>	Public Building Service	<b>SME PED</b>	Secure Mobile Environment Portable Electronic Device
<b>PBX</b>	Private Branch Exchanges	<b>SOC</b>	Security Operations Center
<b>PDD</b>	Presidential Decision Directive	<b>SP</b>	Special Publication
		<b>SPP</b>	Security & Prosperity Partnership
		<b>SRM</b>	Service Component Model
		<b>SS7</b>	Signaling System 7
		<b>SA</b>	Situational Awareness
		<b>SSA</b>	Social Security Administration
		<b>SSP</b>	Sector Specific Plan (Section III)
		<b>SSP</b>	System Security Plans (Section IV)
		<b>STE</b>	Secure Terminal Equipment

STU  
SVDC  
SVP-COI

Secure Telephone Unit  
Secure Video and Data Collaboration  
Secure Voice Products Community  
of Interest  
Secure Video Teleconferencing

SVTC

X

XTE  
XCCDF

eXperimental Testbed Environment  
Extensible Configuration Checklist  
Description Format

T

TADAC

Technology Assessment and Data  
Analysis Cell

TAN

Technology Assessment Network

TCA

Transformational Communications  
Architecture

TCS

Treasury Communications System

TEDE

Telecommunications Electromagnetic  
Disruptive Effects

TEPITF

Telecommunications and Electric Power  
Interdependencies Task Force

TRM

Technical Reference Model

TSC

Telecommunications Service Center

TSP

Telecommunications Service Priority

TSS

Technical Security and Safeguards

TTX

Test, Training, and Exercises

U

USDA

U.S. Department of Agriculture

USMS

United States Marshals Service

USPS

U.S. Postal Service

V

VA

Department of Veterans Affairs

VANTS

VA Nationwide Teleconferencing System

VoIP

Voice over Internet Protocol

VPN

Virtual Private Network

W

WARN

Warning, Alert, and Response  
Network Act

WP

Work Program

WPO

Wireless Program Office

WPS

Wireless Priority Service

WS

Wireless Services Section



## Photo Credits



### Section I Divider – page 1

1960'S—Strategic Air Command personnel interpreting reconnaissance photo during the Cuban Missile Crisis, 1962. (U.S. Air Force photo)



### Section II Divider – page 7

Washington, DC, September 11, 2008—President George Bush (upper left) participates in a Video Tele-Conference (VTC) at FEMA's National Response Coordination Center (NRCC), on preparedness for Hurricane Ike . The VTC is with local, state and federal emergency management teams, via the FEMA network. (Photo by Barry Bahler/FEMA)



### Section III Divider – page 11

Communication Tower  
(Source: iStockphoto® – file# 2318389)



**Section IV Divider – page 49**

Houston, Texas, September 20, 2008—Disaster victims of Hurricane Ike wait patiently at a Disaster Recovery Center (DRC) to register for help. The Federal Emergency Management Agency (FEMA) opens offices in communities hit by disasters to provide “one stop” visits to FEMA and its State, Federal, and Volunteer Agency partners. (Photo by Leif Skoogfors/FEMA)

**Note**—Unless indicated all other images were obtained from a stock image library.

**National Communications System  
Department of Homeland Security**

245 Murray Lane  
Mailstop 0615  
Washington, DC 20598-0615

[www.ncs.gov](http://www.ncs.gov)  
[ncsweb1@dhs.gov](mailto:ncsweb1@dhs.gov)



National  
Communications  
System